Serie Prestige 660HW

Router ADSL2+ con interfaz Wireless 802.11g - RoHS

Manual de Usuario

Versión 3.40



Capítulo 1
Conociendo su Router P660HW

Este capítulo describe las cualidades y aplicaciones de su Prestige.

1.1 Introducción Router Prestige

Su Prestige P660HW-D1 integra una interfaz LAN de 10/100 Mbps autonegociables y un puerto ADSL de alta velocidad. El Prestige es ideal para navegar a alta velocidad y realizar conexiones LAN-to-LAN a redes remotas. El Prestige es un router ADSL compatible con los estándares ADSL/ADSL2/ADSL2+. Las tasas de datos máximas alcanzables por cada estándar se indican en la siguiente tabla. Asimismo, este equipo cumple con la nueva directiva europea RoHS (Restriction of Hazardous Substances).

DATA RATE / STANDARD	UPSTREAM	DOWNSTREAM
ADSL	832 kbps	8Mbps
ADSL2	3.5Mbps	12Mbps
ADSL2+	3.5Mbps	24Mbps

El estándar soportado por su ISP determina las velocidades máximas alcanzables en los canales de subida y bajada. Las velocidades alcanzables dependerán igualmente de la distancia a la central, el ruido, la calidad de la línea, etc.

Integrando DSL y NAT, el Prestige proporciona una sencilla instalación y acceso a Internet. El Prestige es igualmente una completa solución de seguridad que incluye Wi-Fi Protected Access (WPA).

La “H” indica que el dispositivo cuenta con un switch de 4 puertos integrado, y la “W” indica que incluye una tarjeta wireless. El Prestige 660HW-D1 proporciona conectividad Wireless LAN 802.11g permitiendo a los usuarios el disfrutar de la movilidad de trabajar en cualquier lugar dentro del área de cobertura.

Los modelos terminados en “1”, por ejemplo P660HW-D1, indican que el dispositivo trabaja sobre líneas telefónicas analógicas, RTB (Red Telefónica Básica). Los modelos terminados en “3” indican que el

dispositivo trabaja sobre líneas RDSI. Los modelos terminados en “7” indican que el dispositivo trabaja sobre líneas T-RDSI (UR-2).

Utilice únicamente versiones de firmware para su modelo de router Prestige específico. Consulte la etiqueta colocada en la parte inferior de su Prestige.

El configurador gráfico basado en web proporciona una gran facilidad en las tareas de gestión y configuración.

1.2 Cualidades del Prestige.

La siguiente tabla muestra las facilidades de la serie Prestige. Estas facilidades pueden variar en función del modelo. Esta tabla únicamente contiene las funcionalidades más relevantes de la serie Prestige. Por favor, consulte la descripción de características presente más abajo para tener más detalles al respecto.

Algunas funcionalidades no están disponibles en todos los modelos. Consulte con la tabla siguiente para comprobar que características son específicas de su modelo Prestige.

Tabla 1-1 Características Específicas

Modelo / Características	P660HW
Switch de 4 puertos	o
LAN Ethernet 10/100M Auto-crossover	o
Botón reset	o
Interruptor de alimentación	o
Seguridad de red 802.1x	o
Redirección de tráfico	o
Políticas de enrutamiento IP	o
UPnP	o
Gestión remota	o

Log centralizado	o
Wi-Fi Protected Access (WPA)	o

- **Acceso a Internet de alta velocidad**

Su router Prestige ADSL/ADSL2/ADSL2+ puede soportar tasas en el canal de bajada de hasta 24Mbps en flujo de bajada y hasta 3.5Mbps en el de subida.

- **IEEE 802.11g 54Mbps Wireless LAN**

El estándar IEEE 802.11g es totalmente compatible con el estándar IEEE 802.11b. Esto indica que una tarjeta inalámbrica IEEE 802.11b puede conectarse directamente con un punto de acceso IEEE 802.11g (y viceversa) a una tasa de 11Mbps o inferior en función del rango. El estándar IEEE 802.11g tiene varias tasas de transmisión intermedias entre la tasa máxima y la mínima. La tasa de transmisión y la modulación para el IEEE 802.11g son como se indica:

IEEE 802.11g	
TASA DE TRANSFERENCIA (Mbps)	**MODULACIÓN**
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5/11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

El Prestige puede ser susceptible a interferencias RF (Radiofrecuencia) por la presencia de otros dispositivos que trabajen en el entorno de los 2.4GHz como los hornos microondas, teléfonos inalámbricos, dispositivos Bluetooth y cualquier otro dispositivo Wireless LAN.

- **Filtrado de direcciones MAC en interfaz Wireless**

Su Prestige puede chequear las direcciones MAC de las estaciones inalámbricas frente a una lista de direcciones MAC permitidas o prohibidas.

- **Encriptación WEP**

WEP (Wired Equivalent Privacy) encripta los paquetes de datos antes de su transmisión sobre el canal radio para ayudar a mantener la privacidad de la comunicación.

- **Wi-Fi Protected Access**

Wi-Fi Protected Access (WPA) es un subconjunto del draft IEEE 802.11i. Las principales diferencias entre WPA y WEP son la autenticación de los usuarios y la mejora en la encriptación de los datos.

- **Redirección del Tráfico**

La redirección del tráfico remite el tráfico WAN hacia un gateway de backup en la parte LAN cuando el Prestige no puede conectarse a Internet, esto actúa como un backup auxiliar cuando la conexión WAN habitual falla.

- **Universal Plug and Play (UPnP)**

Utilizando el protocolo estándar TCP/IP, el Prestige y otros dispositivos UPnP pueden constituir dinámicamente una red, obtener una dirección IP y ofrecer sus servicios a otros dispositivos de la red.

- **Soporte PPPoE (RFC2516)**

PPPoE (Point-to-Point Protocol over Ethernet) emula una conexión Dial-Up. Esto permite a su ISP usar su configuración de red existente con las últimas tecnologías de ancho de banda, como es el caso de ADSL. El driver PPPoE en el Prestige es transparente a los ordenadores de la LAN, la cuál solo ve Ethernet y no se preocupa del PPPoE lo que permite no tener que configurar clientes PPPoE en los distintos ordenadores.

- **Network Address Translation (NAT)**

El NAT permite la traslación de una dirección IP utilizada en una red (por ejemplo una dirección IP privada utilizada en una red local) a una dirección IP diferente conocida en otra red (por ejemplo una dirección IP pública utilizada en Internet).

- **Interfaz Ethernet/Fast Ethernet 10/100M Auto-Negociación**

La característica de auto negociación permite al Prestige detectar la velocidad de conexiones entrantes y ajustarla apropiadamente sin intervención manual. Esta característica permite transferencia de datos tanto a 10Mbps como a 100Mbps en ambos modos, half-duplex o full-duplex dependiendo de su red Ethernet.

- **Interfaz Ethernet 10/100Mbps Auto-Crossover (MDI/MDIX)**

Estas interfaces se ajustan automáticamente bien a un cable Ethernet recto o cruzado.

- **Soporte Dynamic DNS**

Con Dynamic DNS (DNS dinámica), usted puede disponer de un alias estático para una dirección IP dinámica, permitiendo que ese interfaz pueda ser accedido de forma sencilla desde Internet. Para hacer uso de este servicio es necesario registrarse con un proveedor de servicios de DNS Dinámico.

- **Soporte de múltiples circuitos virtuales permanentes, PVC (Permanent Virtual Circuits)**

Su Prestige soporte hasta 8 PVC’s.

- **Ratios de transmisión estándar ADSL**

  - Full-Rate (ANSI T1.413, Issue 2; G.dmt (G.992.1) con soporte de un ratio de línea de hasta 8Mbps en el flujo de bajada y 832Kbps en el flujo de bajada.
  - G.lite (G.992.2) con soporte de un ratio de hasta 1.5Mbps en el flujo de bajada y 512Kbps en el flujo de subida.
  - Soporta estándar Multi-Mode (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2)).
  - Protocolo TCP/IP (Transmission Control Protocol/Internet Protocol).
  - ATM Forum UNI 3.1/4.0 PVC.
  - Soporta hasta 8 PVCs (UBR, CBR, VBR).
  - Multiprotocolo sobre AAL5 (RFC 1483).
  - PPP sobre AAL5 (RFC 2364).
  - PPP sobre Ethernet sobre AAL5 (RFC 2516).
  - RFC 1661.

- PPP sobre PAP (RFC 1334).
- PPP sobre CHAP (RFC 1994).

Protocolos soportados

- Soporte DHCP

  DHCP (Dynamic Host Configuration Protocol) permite a los clientes (ordenadores) obtener la configuración TCP/IP desde un servidor DHCP centralizaco. El prestige ha sido diseñado para poder actuar como servidor DHCP, opción activada por defecto. Este puede asignar direcciones IP, una puerta de enlace por defecto y servidores DNS a clientes DHCP. Además, ahora el Prestige también actúa como un sustituto del servidor DHCP (DHCP Relay) donde éste transmite direcciones IP asignadas desde el servidor DHCP real hacia los clientes.

- IP Alias

  IP Alias le permite participar una red física en redes lógicas sobre la misma interfaz Ethernet. El Prestige soporta tres interfaces LAN lógicas sobre un interfaz Ethernet simple, con el mismo Prestige como puerta de enlace para cada red LAN.

- Política de enrutado IP (IPPR)

  Tradicionalmente, el enrutado se basa sólo en direcciones destino y el router toma el camino más corto para dirigir un paquete. La política de enrutado IP (IPPR) proporciona un mecanismo para cambiar el comportamiento por defecto en el enrutado y alterar el direccionamiento de paquetes, basándose en la política definida por el administrador de red.

- Protocolo PPP (Point-to-Point Protocol).
- Birdge transparente para protocolos sin soporte en capa de red.
- RIP I/RIP II
- IGMP Proxy
- Soporta ICMP
- Soporta ATM QoS (Quality of Service)
- Soporta MIB II (RFC 1213)

- **Compatibilidad en Red**

Su prestige es compatible con la mayoría de proveedores DSLAM (Digital Subscriber Line Access Multiplexer) ADSL, haciendo de la configuración lo más simple posible para usted.

- **Multiplexado**

Las series Prestige soportan multiplexado basado en VC (VC-based) y basado en LLC (LLC-based).

- **Encapsulación**

Las series Prestige soportan PPPoA (RFC 2364 - PPP sobre ATM Adaptation Layer 5), encapsulación RFC 1483 sobre ATM, encapsulado enrutado en MAC (ENET encapsulation) y también PPP sobre Ethernet (RFC 2516).

- **Gestión de red**

  - Gestión por el menú SMT (System Management Terminal)
  - Configurador Web
  - CLI (Command Line Interpreter)
  - Gestión remota via Telnet o Web
  - Gestión SNMP
  - Servidor/Cliente/Relay DHCP
  - Herramientas de diagnóstico incorporadas
  - Syslog
  - SoporteTelnet (Acceso al configurador protegido con password)
  - Servidor TFTP/FTP, soporte de actualización del firmware y actualización/backup de la configuración
  - Soporta celdas OAM F5 loop-back, AIS y celdas RDI OAM

- **Otras características PPPoE**

  - Temporizador sesión PPPoE

- ♦ Establecimiento sesión PPPoE bajo de demanda

- **Capacidades de diagnóstico**

El Prestige puede realizar autotests de diagnóstico. Estos tests comprueban la integridad de los siguientes componentes

- ♦ Memoria FLASH
- ♦ Circuitería ADSL
- ♦ RAM
- ♦ Puertos LAN

- **Filtrado de paquetes**

Las funciones de filtrado de paquetes del Prestige añaden facilidades en la seguridad y gestión de red.

- **Facilidad en la instalación**

Su Prestige está diseñado para una rápida, intuitiva y fácil instalación.

- **Housing**

El formato compacto de su Prestige así como el ventilado habitáculo, minimiza requerimientos de espacio, haciendo de este fácil de posicionar en cualquier lugar.

1.3 Aplicaciones para el Prestige

1.3.1 Acceso a Internet

El Prestige es la solución ideal para el acceso a Internet a alta velocidad. Su prestige soporta el protocolo TCP/IP, el cual usa Internet exclusivamente. Es compatible con la mayoría de proveedores de DSLAM DSLAM (Digital Subscriber Line Access Multiplexer) ADSL. Un DSLAM es un rack de tarjetas de líneas ADSL con multiplexado de datos en una interfaz/conexión de red a backbone (ej., T1, OC3, DS3, ATM o Frame Relay). Equivalente a un rack de módems para ADSL. Adicionalmente, el Prestige 660W/HW permite que los clientes wireless puedan acceder a los recursos de red disponibles. Una típica aplicación de acceso a Internet se muestra a continuación.

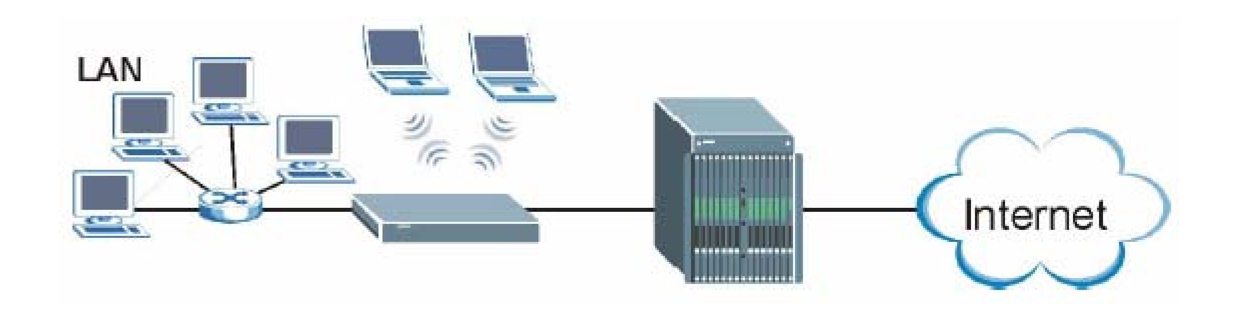


Figura 1-1 Aplicación de acceso a Internet

Cuenta individual de usuario de acceso a Internet

Pensado para entornos SOHO (Small Office/Home Office), su Prestige ofrece la característica de cuenta de usuario simple, Single User Account (SUA), la cual permite a múltiples usuarios de la LAN (Local Area Network) acceder a Internet concurrentemente con el coste de una dirección IP simple.

1.3.2 Aplicación LAN-to-LAN

Puede usar el Prestige para conectar dos redes geográficamente dispersas sobre una línea ADSL. A continuación se muestra una aplicación típica LAN-to-LAN para su Prestige.

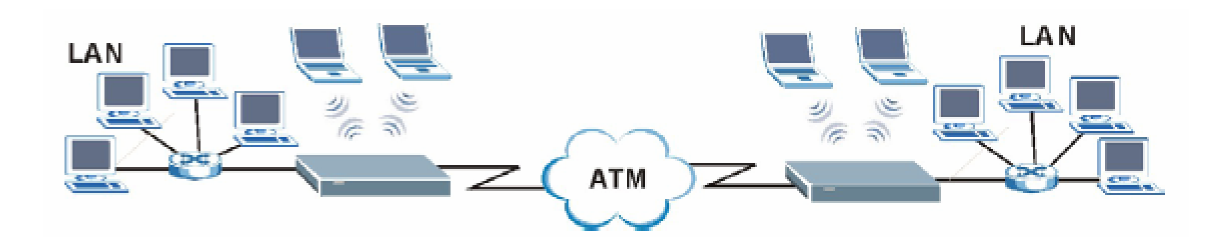


Figura 1-3 Aplicación LAN-to-LAN

Capítulo 2
Introducción al Configurador Web

Este capítulo describe como acceder y navegar por el configurador web.

2.1 Descripción del Configurador Web

El configurador web integrado le permite gestionar el Prestige desde cualquier ubicación a través de un navegador web tal como Microsoft Internet Explorer o Netscape Navigator. Utilice al menos Internet Explorer 6.0 y posteriores o Netscape Navigator 7.0 y posteriores con JavaScript habilitado. Se recomienda configurar la resolución de pantalla a 1024x768 píxeles.

2.2 Accediendo al configurador Web del Prestige

Paso 1. Asegúrese que las conexiones hardware del Prestige están correctamente hechas (consulte la *Guía Rápida*).

Paso 2. Prepare su ordenador/adaptador de red para conectarse con su Prestige (consulte la *Guía Rápida*).

Paso 3. Lance su navegador web.

Paso 4. Introduzca “192.168.1.1” en la dirección URL.

Paso 5. Aparecerá una ventana para introducir los parámetros de acceso al equipo. Introduzca el username (“1234” por defecto), la password (“1234” por defecto) y pulse sobre **OK**.

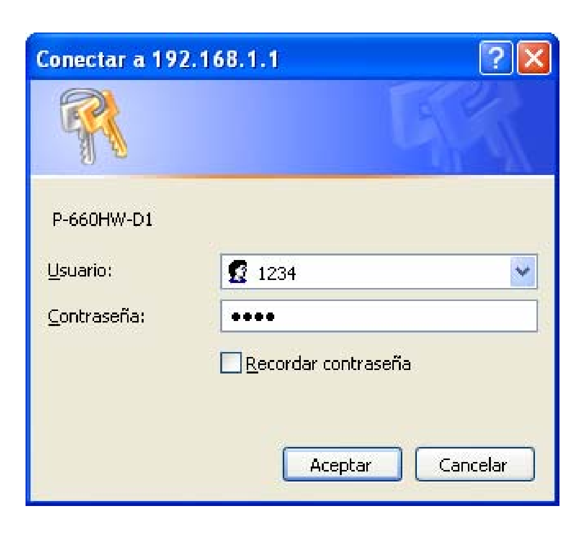


Figura 2.1 – Pantalla de acceso

Paso 6. Ahora debería visualizar la pantalla principal del configurador.

El Prestige automáticamente cerrará la sesión tras cinco minutos de inactividad. Deberá introducir nuevamente los parámetros de acceso para registrarse y volver a acceder al equipo.

2.3 Resetear el Prestige

Si olvida su contraseña de acceso o no puede acceder al configurador web, necesitará utilizar el botón **RESET** situado en el panel posterior del Prestige para cargar los parámetros de la configuración por defecto. Con esto, perderá toda la configuración que tuviese previamente el equipo y la contraseña volverá a ser “1234”.

2.3.1 Utilización del Botón de Reset

Paso 1. Asegúrese que el LED **SYS** o **PWR/SYS** está encendido (sin parpadear).

Paso 2. Presione el botón RESET durante unos 10 segundos o hasta que el LED **SYS** o **PWR/SYS** comience a parpadear, en ese momento deje de presionar. Cuando el LED **SYS** o **PWR/SYS** empiece a parpadear, los parámetros por defecto han sido restaurados y el Prestige se reiniciará.

2.4 Navegando por el Configurador Web

A continuación se muestra como navegar por el configurador web a partir de la pantalla del menú principal. Utilizaremos las pantallas del Prestige P660HW-D1 como ejemplo para esta guía. Las pantallas pueden variar ligeramente para los diferentes modelos.

- Pulse sobre **Wizard Setup** para lanzar una serie de pantallas para configurar su Prestige por primera vez.
- Pulse sobre cualquier opción bajo el enunciado **Advanced Setup** para configurar funcionalidades avanzadas del Prestige.
- Pulse sobre cualquier enlace bajo el enunciado **Maintenance** para visualizar estadísticas de funcionamiento, actualizar el firmware del equipo, hacer backups o restauraciones del fichero de configuración del Prestige.
- Pulse sobre **Site Map** para ir a la pantalla del menú principal.
- Pulse sobre **Logout** cuando haya finalizado su sesión de gestión del Prestige.



Figura 2-2 Pantalla principal del Configurador Web

Pulse sobre el icono HELP (situado en la esquina superior derecha de la mayoría de las pantallas) para visualizar la ayuda integrada.

Tabla 2-1 Resumen de Pantallas del Configurador Web

ENLACE	SUB-ENLACE	FUNCIÓN
Wizard Setup		Utilice estas pantallas para la configuración inicial que incluye la configuración general de parámetros del equipo, parámetros ISP para el acceso a Internet y la asignación de direcciones IP de WAN.
Advanced Setup		
Password		Utilice esta pantalla para cambiar la contraseña
LAN		Utilice esta pantalla para configurar los parámetros DHCP y TCP/IP de la interfaz LAN.
WIRELESS LAN	Wireless	Utilice esta pantalla para configurar los parámetros wireless.
	MAC Filter	Utilice esta pantalla para modificar los parámetros de filtrado MAC en el Prestige.
	802.1x	Utilice esta pantalla para configurar los parámetros de autenticación WLAN.
	Local User Database	Utilice esta pantalla para configurar las cuentas de usuario locales.
	RADIUS	Configure esta pantalla para utilizar un servidor externo para autenticación wireless.
WAN	WAN Setup	Utilice esta pantalla para cambiar los parámetros del nodo remoto WAN
	WAN Backup	Utilice esta pantalla para configurar las propiedades de la redirección de tráfico y los parámetros del backup de WAN
NAT	SUA Only	Utilice esta pantalla para configurar los servidores tras el Prestige
	Full Feature	Utilice esta pantalla para configurar reglas de traslación de direcciones de red
Security		Utilice esta pantalla para filtrar el acceso desde el exterior a determinados tipos de tráfico.

Dynamic DNS		Utilice esta pantalla para configurar el DNS Dinámico
Time and Date		Utilice esta pantalla para modificar los parámetros de fecha y hora de su Prestige
Remote Management		Utilice esta pantalla para configurar a través de que interfaz o interfaces y desde que direccion(es) IP de usuario se puede utilizar Telnet/FTP/Web para gestionar el Prestige
UPnP		Utilice esta pantalla para habilitar el UPnP en el Prestige
Logs	Log Settings	Utilice esta pantalla para cambiar las categorías a registrar por el Prestige.
	View Log	Utilice esta pantalla para visualizar los logs de las categorías seleccionadas
Media Bandwidth Management	Summary	Utilice esta pantalla para reservar en los distintos interfaces determinado ancho de banda saliente
	Class Setup	Utilice esta pantalla para definir las clases
	Monitor	Utilice esta pantalla para visualizar estadísticas
Maintenance		
System Status		Esta pantalla contiene información administrativa y relativa al sistema.
DHCP Table		Esta pantalla muestra información relativa al DHCP (solo lectura).
Wireless LAN	Association List	Esta pantalla muestra la dirección(es) MAC de las estaciones wireless que actualmente está asociadas en la red
Diagnostic	General	Estas pantallas muestran información para ayudar a identificar problemas con la conexión general del Prestige
	DSL Line	Estas pantallas muestran información para ayudar a identificar problemas con la línea ADSL.
Firmware		Utilice esta pantalla para actualizar el firmware del Prestige
LOGOUT		Pulse sobre esta etiqueta para salir del configurador web.

Capítulo 3
Asistente de Configuración

Este capítulo mostrará información sobre las pantallas del Asistente de Configuración del Configurador Web.

3.1 Introducción al Asistente de Configuración

Utilice el Asistente para configurar su sistema con los parámetros adecuadaos de Acceso a Internet.

3.2 Encapsulación

Asegurese de utilizar elmétodo de encapsulación requerido por su ISP. El Prestige soporta los métodos siguientes.

3.2.1 ENET ENCAP

El ‘MAC Encapsulated Routing Link Protocol’ (ENET ENCAP), está solamente implementado con el protocolo de red IP. Los paquetes IP son enrutados entre la interfaz Ethernet y la interfaz WAN, después de tener la ruta establecida, éstos pueden ser comprendidos en un entorno de bridge, ej. éste encapsula frames Ethernet enrutados dentro de celdas ATM por bridge. ENET ENCAP requiere que especifique una dirección IP como puerta de enlace en el campo **Ethernet Encapsulation Gateway** en el Menú 4 y en el campo **Rem IP Addr** en el Menú 11.1. Puede obtener esta información de su ISP.

3.2.2 PPP sobre Ethernet

PPPoE provee control de acceso y funcionalidad de facturación en un modo similar a los servicios dial-up usando PPP. El Prestige hace bridge a una sesión PPP sobre Ethernet (PPP over Ethernet, RFC 2516) desde

su ordenador a un ATM PVC (Permanent Virtual Circuit), circuito virtual permanente ATM, el cual conecta a un concentrador de acceso xDSL donde la sesión PPP tiene su fin. Un PVC puede soportar cualquier número de sesiones PPP desde su LAN. Para más información acerca de PPPoE vea los Apendices.

3.2.3 PPPoA

Por favor consulte el RFC 2364 para más información en cuanto a ‘PPP over ATM Adaptation Layer 5 (AAL5)’. Consulte el RFC 1661 para más información sobre PPP

3.2.4 RFC 1483

El RFC 1483 describe metodos para encapsulación multiprotocolo sobre adaptación de capa 5 ATM (AAL5). El primer método permite multiplexar múltiples protocolos sobre un circuito virtual ATM simple (multiplexado basado en LLC) y el segundo método asume que cada protocolo es transportado sobre un circuito virtual separado (multiplexado basado en VC). Por favor consulte el RFC para información más detallada.

3.3 Multiplexado

Hay dos convenciones para identificar que protocolos transporta el circuito virtual (VC). Asegurese de usar el método de multiplexado requerido por su ISP.

3.3.1 Multiplexado basado en VC

En este caso, por previo acuerdo mutuo, cada protocolo es asignado a un circuito virtual específico, ej., VC1 transporta IP, VC2 transporta IPX, etc. El multiplexado basado en VC puede ser dominante en entornos donde la creación dinámica de grandes cantidades de VC ATM sea rápida y económica.

3.3.2 Multiplexado basado en LLC

En este caso un VC transporta multiples protocolos con información identificadora de protocoloen la cabecera de cada paquete. A pesar de el ancho de banda extra y del sobreproceso de las cabeceras, este

método puede ser ventajoso si éste no es práctico para tener un VC separado para cada protocolo transportado, ej. si la carga depende fuertemente número de VCs simultáneos.

3.4 VPI y VCI

Asegurese de usar los números correctos, que le hayan sido proveidos por su companyia telefónica, para el identificador de camino virtual, Virtual Path Identifier (VPI), y el identificador de canal virtual, Virtual Channel Identifier (VCI). El rango válido para el VPI es de 0 a 255 y para el VCI de 32 a 65535 (el rango de 0 a 31 está reservado para gestión local de tráfico ATM). Por favor, mire los Apéndices para más información.

3.5 Asistente de Configuración : Primera pantalla

En la pantalla principal del menú, pulse sobre **Wizard Setup** para mostrar la primera pantalla del Asistente.

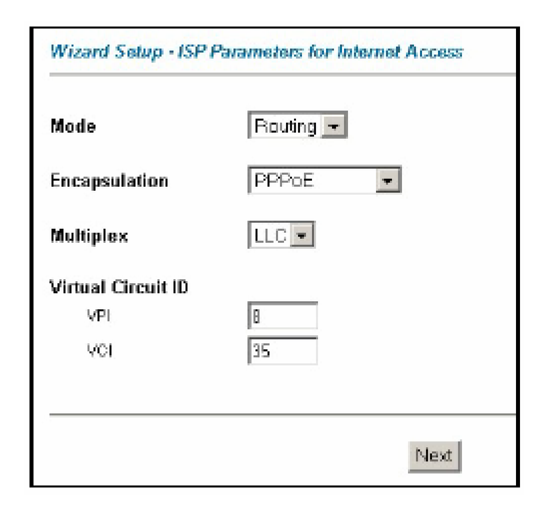


Figure 3-1 Pantalla 1 del Asistente

La siguiente tabla describe los campos de esta pantalla.

Tabla 3-1 Pantalla 1 del Asistente

ETIQUETA	DESCRIPCIÓN
Mode	Desde la lista desplegable **Mode**, seleccione **Routing** (por defecto) si su ISP a múltiples ordenadores compartir el acceso a Internet. De otra forma seleccione **Bridge**.
Encapsulation	Seleccione el tipo de encapsulación utilizado por su ISP de la lista desplegable **Encapsulation**. Las opciones dependerán de lo que se seleccione en el campo **Mode**.
Multiplex	Seleccione el método de multiplexación utilizado por su ISP de la lista desplegable **Multiplex**, bien VC-based o LLC-based
Virtual Circuit ID	VPI(Virtual Path Identifier) y VCI(Virtual Circuit Identifier) definen un circuito virtual. Consulte el apéndice para más información.
VPI	Introduzca el VPI que le indique su ISP.
VCI	Introduzca el VCI que le indique su ISP.
Next	Pulse sobre este botón para ir a la siguiente pantalla del asistente. La siguiente pantalla dependerá del protocolo seleccionado.

3.6 Dirección IP y máscara de subred

Como las casas en las calles, que comparten un nombre de calle común, las máquinas en una LAN comparten un número de red común.

De dónde se obtiene el número de red depende de su situación particular. Si su ISP o su administrador de red le asigna un bloque de direcciones IP registradas, siga sus instrucciones para seleccionar la dirección IP y la máscara de subred.

Si su ISP no le asignó explicitamente un número de red IP, seguramente esté utilizando una cuenta de usuario simple y su ISP le asigna una dirección IP dinámicamente cada vez que establece una conexión. Si este es el caso, se recomienda que seleccione un número de red desde 192.168.0.1 a 192.168.255.0 y que habilite la cuenta de usuario simple (SUA) que le permite el Prestige. La autoridad de assignación de números Internet, Internet Assigned Number Authority (IANA), reserva este bloque de direcciones especificamente para uso privado; por favor no utilice cualquier otro número amenos que se le haya

indicado. Le aconsejamos seleccionar como número de red la IP 192.168.1.0, que cubre 254 direcciones individuales, desde 192.168.1.1 a 192.168.1.254 (0 y 255 estan reservadas). En otras palabras, los tres primeros números especifican el número de red, mientras que el último número identifica una estación de trabajo individualmente en tal red.

La máscara de subred especifica la porción de una dirección IP referida al número de red. Su Prestige completará la máscara de subred automáticamente basandose en la dirección IP que haya introducido. No necesita cambiar la máscara de subred introducida por el Prestige a menos que sea instruido para hacerlo.

3.7 Asignación de direcciones IP

Una IP estática es una IP fija que su ISP le asigna. Una IP dinámica no es fija, su ISP le asigna una diferente cada vez que realiza una nueva conexión. La utilidad de cuenta de usuario simple (SUA) puede ser habilitada para ambas posibilidades. Sin embargo el método de encapsulación asignado influye en su elección para direcciones IP y puerta de enlace ENET ENCAP.

3.7.1 Asignación IP con encapsulación PPPoA o PPPoE

Si usted tiene una IP dinámica, la dirección IP y la puerta de enlace ENET ENCAP no son aplicables (N/A). Si usted tiene una IP estática, sólo necesita rellenar el campo dirección IP y no el campo puerta de enlace ENET ENCAP.

3.7.2 Asignación IP con encapsulación RFC1483

En este caso la dirección IP asignada debe ser estática, con los mismos requerimientos para la dirección IP y la puerta de enlace ENET ENCAP que en el caso anterior.

3.7.3 Asignación IP con encapsulación ENET ENCAP

En este caso usted puede disponer de ambas opciones, IP estática o dinámica. Para una IP estática debe rellenar todos los campos de dirección IP y puerta de enlace ENET ENCAP como le sean suministrados por su ISP. Sin embargo para una IP dinámica, el Prestige actúa como cliente DHCP en el puerto WAN y los campos dirección IP y puerta de enlace ENET ENCAP no son aplicables (N/A), pues son asignados al Prestige por un servidor DHCP.

3.7.4 Direcciones IP privadas

Todas las máquinas en Internet debe tener una dirección única. Si sus redes estan aisladas de Internet, por ejemplo solo entre dos oficinas de su compañía, puede asignar cualquier dirección IP a sus máquinas sin problemas. Sin embargo, la autoridad de asignación de números Internet (IANA) ha reservado los siguientes tres bloques de direcciones IP especificamente para redes privadas:

```
10.0.0.0     -  10.255.255.255

172.16.0.0   -  172.31.255.255

192.168.0.0  -  192.168.255.255
```

Puede obtener su dirección IP de IANA, de un ISP o ser asignada desde un red privada. Si usted pertenece a una pequeña organización y su acceso a Internet es a través de un ISP, el ISP puede proveerle de la dirección Internet para sus redes locales. Por otra parte, si usted es parte de una organización mayor, deberia consultar su administrador de red para obtener las direcciones IP apropiadas.

No asigne una dirección IP arbitrariamente sin tener en cuenta su situación particular; siga siempre las indicaciones del manual. Para más información acerca de la asignación de direcciones, consulte el RFC 1597, *Asignación de direcciones privadas para Internet* y RFC 1466, *Guia para gestionar el espacio de direcciones IP*.

3.8 Conexión Nailed-Up (PPP)

Una conexión nailed-up es una línea dial-up donde la conexión está siempre establecida sin hacer caso de la demanda de tráfico. Su Prestige realiza dos acciones cuando usted especifica una conexión nailed-up. La primera es que se deshabilita el temporizador por inactividad (idle timeout). La segunda consiste en que el Prestige intentará activar la conexión cuando se conecta la primera vez o siempre que vea la conexión caída.

No active una conexión nailed-up a menos que su compañía telefónica le ofrezca una tarifa plana o que usted necesite una conexión constantemente establecida sin importarle el coste.

3.9 NAT

NAT (Network Address Translation - NAT, RFC 1631 - Traslación de dirección de red) es la traslación de la dirección IP de una máquina en un paquete, por ejemplo, sería cambiar la dirección origen de un paquete saliente, usada en una red por una dirección IP diferente conocida dentro de otra red.

3.10 Asistente de Configuración : Segunda pantalla

La segunda pantalla del asistente dependerá del modo y la encapsulación seleccionadas en la pantalla anterior. Todas las pantallas mostradas aparecen con modo routing. Configure estos campos y pulse sobre **Next** para continuar.

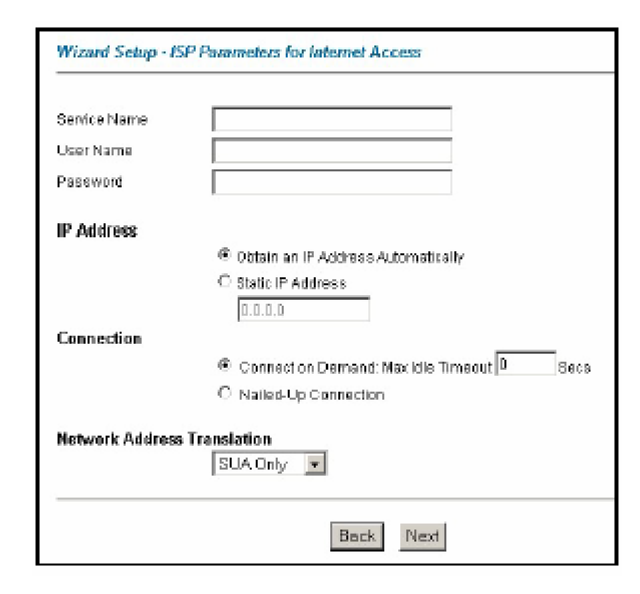


Figura 3-2 Conexión a Internet con PPPoE

La siguiente tabla describe los campos de esta pantalla.

Tabla 3-2 Conexión a Internet con PPPoE

ETIQUETA	DESCRIPCIÓN
Service Name	Introduzca aquí el nombre de su servicio PPPoE
User Name	Introduzca el nombre de usuario asignado por su ISP.
Password	Introduzca el password asociado con el nombre de usuario tecleado arriba.
IP Address	Una dirección IP estática es una dirección fija asignada por su ISP. Una dirección IP dinámica no es fija; el ISP le asignará una dirección IP diferente cada vez que se conecte a Internet. La funcionalidad de Cuenta de Usuario Única (SUA) puede ser utilizada tanto con una dirección estática como dinámica. Seleccione **Obtain an IP Address Automatically** si tiene una dirección IP dinámica; de cualquier otra forma, seleccione **Static IP Address** e introduzca la dirección IP asignada por su ISP en el campo **IP Address** situado más abajo.
Connection	Seleccione **Connect on Demand** cuando no desee que la conexión esté siempre levantada y especifique un temporizador de inactividad (en segundos) en el campo **Max. Idle Timeout**. Por defecto aparece el campo **Connection on Demand** seleccionado con un temporizador de 0, lo que indica que la sesión internet no caerá nunca por inactividad.
Network Address Translation	Seleccione **None, SUA Only** o **Full Feature** de la lista desplegable. Consulte el capítulo NAT para más detalles.
Back	Pulse **Back** para volver a la primera pantalla del asistente.
Next	Pulse **Next** para pasar a la siguiente pantalla.

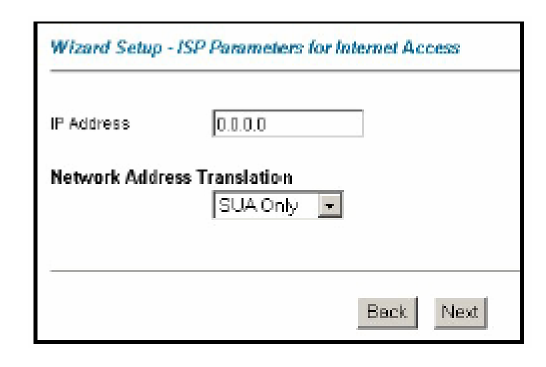


Figura 3-3 Conexión a Internet con RFC1483

La siguiente tabla describe los campos de esta pantalla.

Tabla 3-3 Conexión a Internet con RFC1483

ETIQUETA	DESCRIPCIÓN
IP Address	Este campo aparecerá si selecciona **Routing** en el campo **Mode**.
Network Address Translation	Seleccione **None, SUA Only** o **Full Feature** de la lista desplegable. Consulte el capítulo NAT para más detalles.
Back	Pulse **Back** para volver a la primera pantalla del asistente.
Next	Pulse **Next** para pasar a la siguiente pantalla.

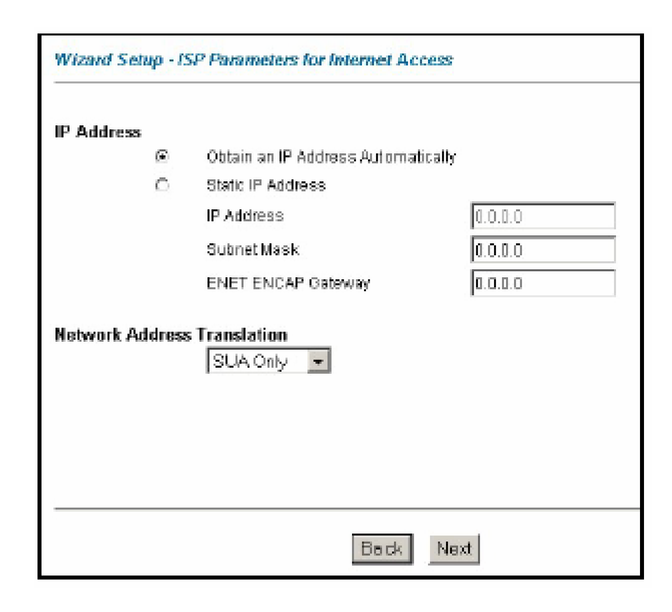


Figura 3-4 Conexión a Internet con ENET ENCAP

La siguiente tabla describe los campos de esta pantalla.

Tabla 3-4 Conexión a Internet con ENET ENCAP

ETIQUETA	DESCRIPCIÓN
IP Address	Una dirección IP estática es una dirección fija asignada por su ISP. Una dirección IP dinámica no es fija; el ISP le asignará una dirección IP diferente cada vez que se conecte a Internet. La funcionalidad de Cuenta de Usuario Única (SUA) puede ser utilizada tanto con una dirección estática como dinámica. Seleccione **Obtain an IP Address Automatically** si tiene una dirección IP dinámica; de cualquier otra forma, seleccione **Static IP Address** e introduzca la dirección IP asignada por su ISP en el campo **IP Address** situado más abajo.
Subnet Mask	Introduzca la máscara de subred en formato decimal. Consulte el apéndice de Subredes IP para calcular la máscara de subred.
ENET ENCAP Gateway	Debe especificar la dirección IP del gateway (proporcionado por su ISP) cuando utilice **ENET ENCAP** en el campo **Encapsulation** de la pantalla previa.

Network Address Translation	Seleccione **None, SUA Only** o **Full Feature** de la lista desplegable. Consulte el capítulo NAT para más detalles.
Back	Pulse **Back** para volver a la primera pantalla del asistente.
Next	Pulse **Next** para pasar a la siguiente pantalla.

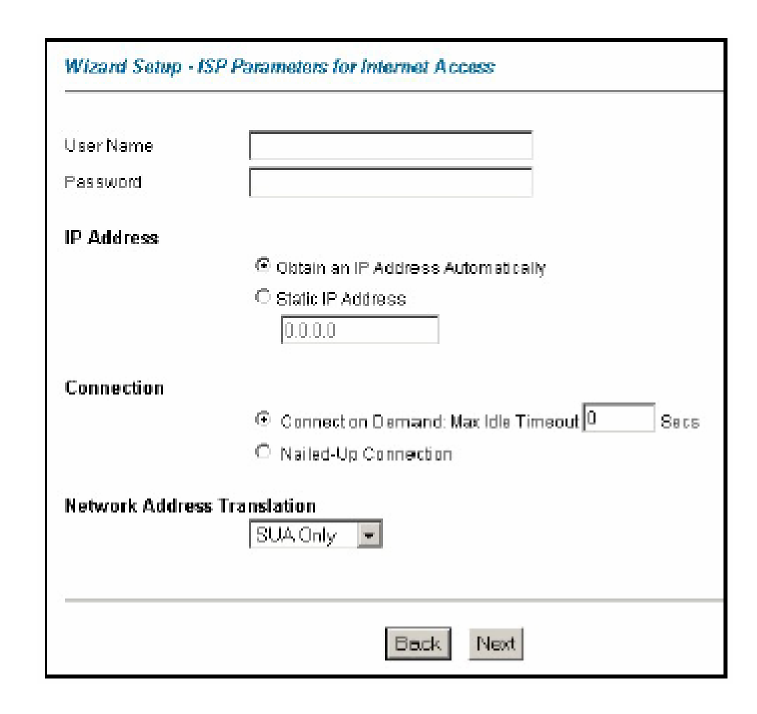


Figura 3-5 Conexión a Internet con PPPoA

La siguiente tabla describe los campos de esta pantalla.

Tabla 3-5 Conexión a Internet con PPPoA

ETIQUETA	DESCRIPCIÓN
User Name	Introduzca el nombre de usuario asignado por su ISP.
Password	Introduzca el password asociado con el nombre de usuario tecleado arriba.

IP Address	Una dirección IP estática es una dirección fija asignada por su ISP. Una dirección IP dinámica no es fija; el ISP le asignará una dirección IP diferente cada vez que se conecte a Internet. La funcionalidad de Cuenta de Usuario Única (SUA) puede ser utilizada tanto con una dirección estática como dinámica. Seleccione **Obtain an IP Address Automatically** si tiene una dirección IP dinámica; de cualquier otra forma, seleccione **Static IP Address** e introduzca la dirección IP asignada por su ISP en el campo **IP Address** situado más abajo.
Connection	Seleccione **Connect on Demand** cuando no desee que la conexión esté siempre levantada y especifique un temporizador de inactividad (en segundos) en el campo **Max. Idle Timeout**. Por defecto aparece el campo **Connection on Demand** seleccionado con un temporizador de 0, lo que indica que la sesión internet no caerá nunca por inactividad.
Network Address Translation	Seleccione **None, SUA Only** o **Full Feature** de la lista desplegable. Consulte el capítulo NAT para más detalles.
Back	Pulse **Back** para volver a la primera pantalla del asistente.
Next	Pulse **Next** para pasar a la siguiente pantalla.

3.11 Configuración DHCP

DHCP (Dynamic Host Configuration Protocol, RFC2131 y RFC2132 - Protocolo de configuración dinámica de equipos) permite a clientes individuales (estaciones de trabajo) obtener la configuración TCP/IP al inicializarse desde un servidor DHCP. Puede configurar el Prestige como servidor DHCP o deshabilitarlo. Cuando se configura como servidor, el Prestige proporciona la configuración TCP/IP a los clientes. Si el servicio DHCP se desactiva, debe disponer de otro servidor DHCP en la LAN o cada ordenador deberá ser configurado manualmente.

3.11.1 Configuración del Pool IP

El Prestige está preconfigurado con un pool de 32 direcciones IP para máquinas cliente, empezando desde la 192.168.1.33 a la 192.168.1.64. Dejando 31 direcciones IP, de la 192.168.1.2 a la 192.168.1.32 (excluyendo la del Prestige, que por defecto es la 192.168.1.1) para otras máquinas servidores, por ejemplo servidores para correo electrónico, FTP, telnet, web, etc., que usted pueda tener.

3.12 Asistente de Configuración : Tercera pantalla

Paso 1. Verifique los parámetros de configuración mostrados. Para cambiar los parámetros de la LAN del Prestige, pulse en **Change LAN Configurations**. En cualquier otro caso, pulse **Save Settings** para guardar la configuración y salte a la sección 3.13.

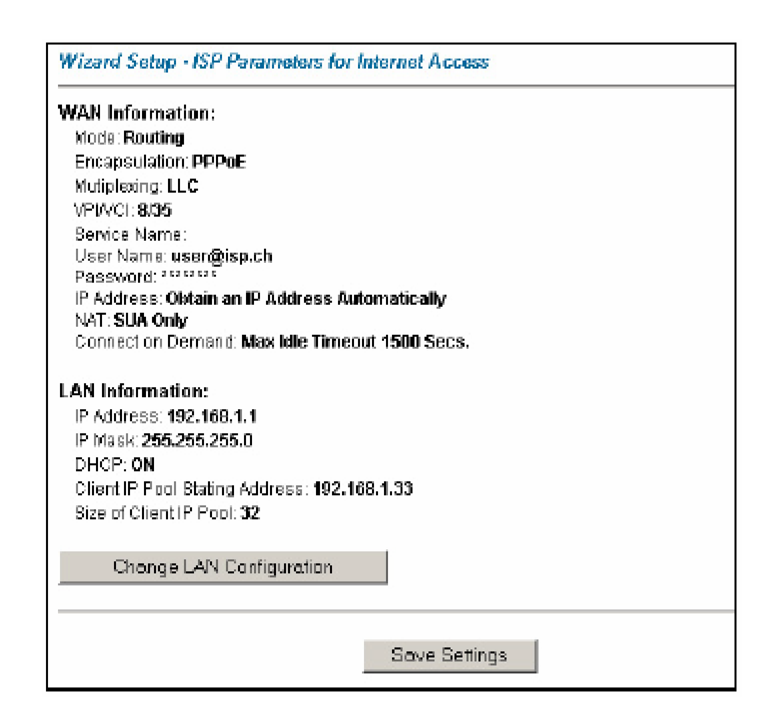


Figura 3-6 Pantalla 3 del Asistente

Paso 2. Si desea modificar los parámetros de la LAN, pulse **Change LAN Configuration** para acceder a la pantalla siguiente.

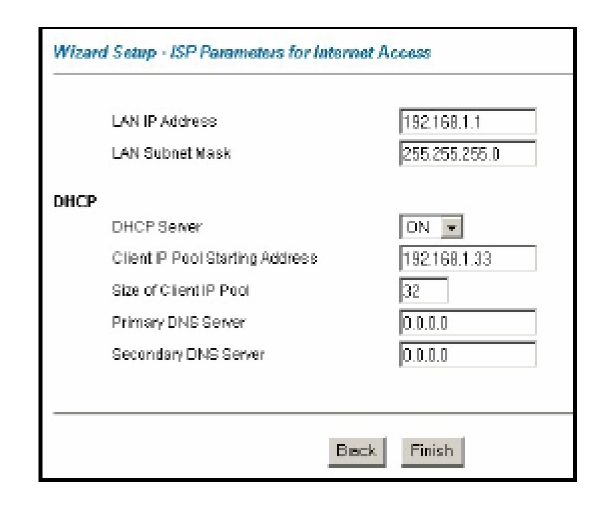


Figura 3-7 Asistente : Configuración LAN

La siguiente tabla describe los campos de esta pantalla.

Tabla 3-6 Asistente : Configuración LAN

ETIQUETA	DESCRIPCIÓN
LAN IP Address	Introduzca la dirección IP de su Prestige en formato decimal, por ejemplo, 192.168.1.1 (por defecto). **Si modifica la dirección IP de la LAN de su Prestige, deberá utilizar la nueva dirección para acceder nuevamente al configurador web.**
LAN Subnet Mask	Introduzca la máscara de subred en formato decimal.
DHCP	
DHCP Server	Desde la lista desplegable **DHCP Server**, seleccione **On** para permitir a su Prestige asignar direcciones IP, puerta predeterminada y servidores DNS a los clientes que soporten cliente DHCP. Seleccione **Off** para deshabilitar el servidor DHCP. Cuando el servidor DHCP está habilitado, configure los siguientes apartados:
Client IP Pool Starting Address	Este campo especifica la primera dirección del pool de direcciones.

Size of Client IP Pool	Este campo especifica el tamaño del pool de direcciones IP.
Primary DNS Server	Introduzca la(s) dirección(es) del servidor DNS. Los servidores DNS se transfieren a los clientes DHCP junto con la dirección IP y la máscara de subred.
Secondary DNS Server	Igual a lo indicado arriba.
Back	Pulse **Back** para volver a la pantalla anterior.
Finish	Pulse **Finish** para guardar la configuración y pasar a la siguiente pantalla.

3.13 Asistente de Configuración : Tests de Conexión

El Prestige automáticamente lleva a cabo verificaciones de la conexión con el/los ordenador(es) conectados a los puertos LAN. Para chequear la conexión desde el Prestige hasta el ISP, pulse **Start Diagnose**. En cualquier otro caso, pulse **Return to Main Menu** para volver a la pantalla principal del configurador web.

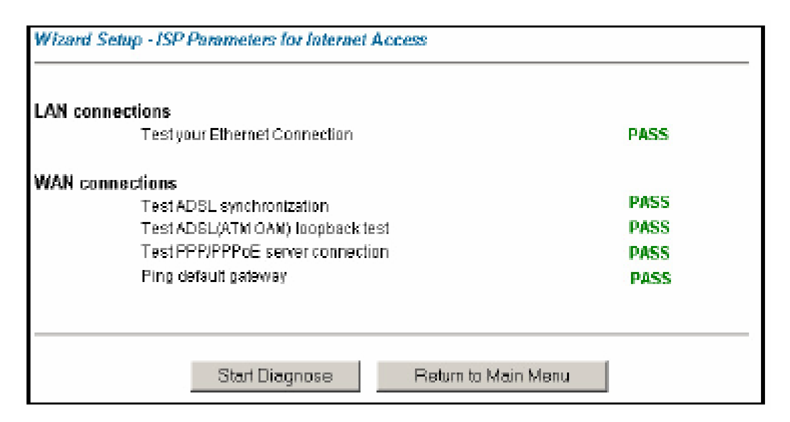


Figura 3-8 Pantalla 4 del Asistente

3.14 Verifique su Conexión a Internet

Lance el navegador web e intente navegar por www.zyxel.com. El acceso a internet es sólo el principio. Consule el resto de esta Guía de Ususario para una información más detallada sobre el conjunto de

funcionalidades del Prestige. Si no puede acceder a Internet, abra nuevamente el configurador web para confirmar que los parámetros de Internet configurados a través del Asistente son correctos.

Capítulo 4
Configuración de Contraseña

Este capítulo proporciona información sobre la pantalla de contraseña de acceso.

.

4.1 Descripción de contraseña

Se recomendienda el cambio de la contraseña configurada por defecto en el Prestige.

4.2 Configuración de la contraseña

Para cambiar la contraseña del Prestige (recomendado), pulse Password. La pantalla que aparece es:

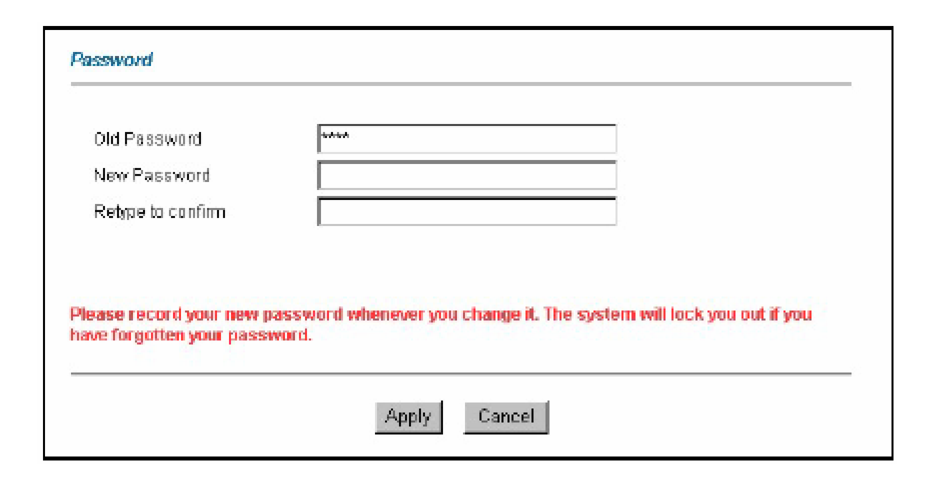


Figura 4-1 Contraseña

La siguiente tabla describe los campos de esta pantalla.

Tabla 4-1 Contraseña

ETIQUETA	DESCRIPCIÓN
Old Password	Introduzca la contraseña que utiliza para acceder al sistema.
New Password	Introduzca la nueva contraseña.
Retype to Confirm	Introduzca la nueva contraseña nuevamente.
Apply	Pulse **Apply** para guardar los cambios en el Prestige.
Cancel	Pulse **Cancel** para comenzar a configurar esta pantalla de nuevo.

Capítulo 5
Configuración LAN

Este capítulo describe como configurar los parámetros de la LAN.

5.1 Descripción de la LAN

Una LAN (Red de Área Local) es un sistema de comunicaciones compartido al que se conectan varios dispositivos. Una LAN es una red de equipos limitada a una zona determinada, usualmente dentro de un edificio o una planta de un edificio. Las pantallas de la LAN le ayudarán a configurar el servidor DHCP de LAN y gestionar las direcciones IP.

5.1.1 LANs, WANs y el Prestige

La conexión física actual determina si los puertos del Prestige son LAN o WAN. Existen dos redes IP separadas, una interior, la red LAN; y otra exterior, la red WAN, como se muestra a continuación:

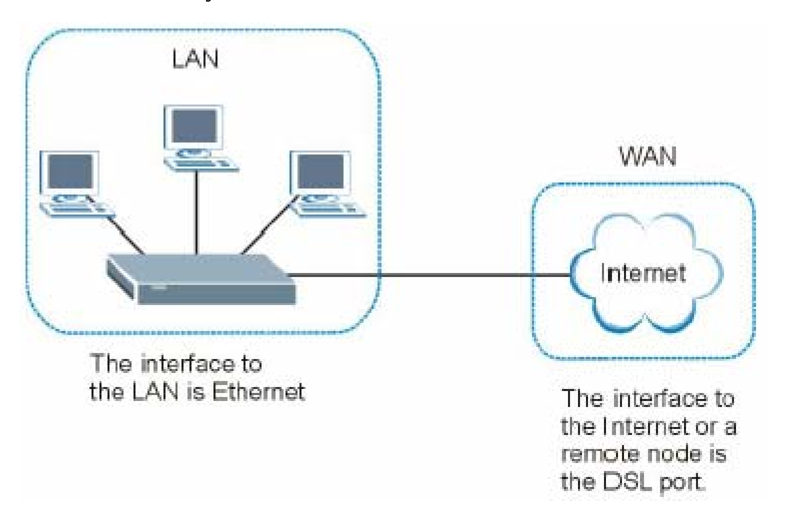


Figura 5-1 Direcciones IP LAN y WAN

5.2 Dirección de Servidores DNS

DNS (Domain Name System - Sistema de nombres de dominio) nos permite mapear un nombre de dominio a su correspondiente dirección IP y viceversa (ej. La dirección IP de www.zyxel.com es 204.217.0.2). El servidor DNS es estremamente importante porque sin él se deberia conocer la dirección IP de una máquina antes de poder acceder a ella. La dirección del servidor DNS que usted entre en la configuración DHCP será pasada a los clientes junto la dirección IP asignada y la máscara de subred.

Hay dos maneras por las cuales un ISP difunde la dirección del servidor DNS. La primera consiste en que el ISP informa a su cliente de la dirección del servidor DNS. Si su ISP le ha informado de la direccion del servidor DNS, introduzcala en el compo **DNS Server** en el **DHCP Setup**, en cualquier otro caso deje este campo en blanco.

Algunos ISP eligen pasar el servidor DNS usando las extensiones PPP IPCP (IP Control Protocol) del servidor DNS una vez la conexión está establecida.. Si su ISP no le asignó ningun servidor DNS explicitamente, posiblemente el servidor DNS sea transmitido en la negociación IPCP. El Prestige soporta las extensiones IPCP de servior DNS a través de la característica de proxy DNS.

Si los campos **Primary** y **Secondary DNS Server** en el **DHCP Setup** no están especificacos (valor 0.0.0.0) el Prestige informa a los clientes que él mismo es el servidor DNS. Cuando un estación de trabajo envia una petición de DNS al Prestige, el Prestige responderá con el servidor DNS real obtenido a través de IPCP.

Tenga en cuenta que el proxy DNS solo funciona cuando el ISP usa las extensiones IPCP de servidor DNS. Esto no quiere decir que pueda dejarse el servidor DNS en blanco en la configuración DHCP bajo cualquier circunstancia. Si su ISP le asigna un servidor DNS explicitamente, asegurese que su dirección IP está correctamente introducida en la configuración DHCP. De este modo, el Prestige puede pasar el servidor DNS a las estaciones de trabajo y éstas podrán localizar el servidor DNS directamente sin la intervención del Prestige.

5.3 Asignación de la dirección del Servidor DNS

Utilice DNS (Domain Name System) para mapear un nombre de dominio con su correspondiente dirección IP y viceversa. El servidor DNS es extremadamente importante porque si él, sería necesario conocer la dirección IP de una máquina para poder acceder a la misma.

Existen dos maneras en las que el ISP informa de la dirección del servidor DNS.

1.- El ISP informa a los clientes de las direcciones de los servidores DNS, normalmente en forma de un documento informativo cuando se da de alta el servicio. Si su ISP le proporciona estas direcciones, introdúzcalas en los campos relativos al Servidor DNS en la configuración del DHCP.

2.- El Prestige actúa como un proxy DNS cuando los campos de servidor DNS Primario y Secundario (**Primary** and **Secondary DNS Server**) se dejan en blanco en la pantalla de configuración de LAN (**LAN Setup**).

5.4 TCP/IP LAN

El Prestige incorpora funcionalidades de servidor DHCP para asignar direcciones IP y direcciones de servidores DNS a los sistemas que tengan habilitadas las capacidades de cliente DHCP.

5.4.1 Parámetros por defecto de LAN

Los parámetros configurados por defecto en la LAN son los siguientes:

- Dirección IP 192.168.1.1 con máscara de subred 255.255.255.0 (24 bits)
- Servidor DHCP habilitado con 32 direcciones IP de cliente comenzando en la 192.168.1.33.

Estos parámetros deberían funcionar en la mayoría de instalaciones. Si su ISP le asigna explícitamente la dirección(es) de los servidores DNS, consulte la ayuda del configurador web integrado para ver como configurar estos campos.

5.4.2 Dirección IP y Máscara de Subred

Consulte la sección de *Dirección IP y Máscara de Subred* en el capítulo **Wizard Setup** (Asistente) para más información.

5.4.3 Configuración RIP

RIP (Routing Information Protocol), protocolo de información de enrutado, permite a un router intercambiar información de enrutado con otros routers. Los campos de dirección RIP, **RIP Direction**, controlan los paquetes RIP enviados y. Cuando se ponen a:

1. **Both -** El Prestige hará un broadcast de su tabla de enrutado periodicamente e incorporará la información RIP recibida.
2. **In Only -** El Prestige no enviará ningún paquete RIP, pero aceptará paquetes recibidos.
3. **Out Only -** El Prestige enviará paquetes RIP, pero no aceptará ningún paquete RIP.
4. **None -** El Prestige no enviará ningún paquete RIP e ignorará cualquierpaqueteRIP recibido.

El campo **Version** controla el formato y el método broadcast de los paquetes RIP que el Prestige envia (éste reconoce ambos formatos al recibir). **RIP-1** es universalmente soportado, pero RIP-2 aporta más información. RIP-1 es provablemente adecuado para la mayoria de redes, a menos que usted tenga una topologia de red inusual.

Tanto **RIP-2B** como **RIP-2M** envian los datos de enrutado en formato RIP-2, la diferencia está en que **RIP-2B** usa broadcast de subred mientras que **RIP-2M** usa multicast.

5.4.4 Multicast

Tradicionalmente, los paquetes IP son transmitidos en uno de los dos posibles modos - Unicast (1 transmisor – 1 receptor) o Broadcast (1 transmisor – todos los equipos de la red). Multicast es un tercer modo de entregar paquetes IP a un grupo de equipos en la red, no a todos los equipos

IGMP (Internet Group Multicast Protocol), es un protocolo de la capa de sesión usado para establecer miembros en un grupo multicast, no se usa para transportar datos de usuario. La version 2 de IGMP (RFC 2236) es una mejora sobre la versión 1 (RFC 1112) pero la versión 1 de IGMP aún se usa ampliamente. Si desea leer más detalladamente información sobre interoperabilidad entre ambas versiones de IGMP, por favor dirijase a las secciones 4 y 5 del RFC 2236. La clase D de direcciones IP se usa para identificar grupos de equipos, puede estar en el rango de 224.0.0.0 a 239.255.255.255. La dirección 224.0.0.0 no se asigna a ningún grupo, es usada para equipos con IP multicast. La dirección 224.0.0.1 es usada para mensajes de petición, se asigna a un grupo permanente que incluye todos las direcciones IP de los equipos (incluyendo puertas de enlace). Todos lo equipos deben compartir el grupo 224.0.0.1 para participar en IGMP. La dirección 224.0.0.2 es asignada para un grupo de routers multicast.

El Prestige soporta ambas versiones IGMP1 (**IGMP-v1** e **IGMP-v2**). Al inicializar, el Prestige busca todas las redes directamente conectadas para unir los miembros del grupo. Después, el Prestige periodicamente actualiza esta información. IP Multicasting puede ser habilitado/deshabilitado en las interfaces LAN y/o

WAN del Prestige usando los menús 3.2 (LAN) y 11.3 (WAN). Seleccione **None** para deshabilitar el multicast IP en estas interfaces.

5.5 Configurando la LAN

Pulse sobre **LAN** para abrir la siguiente pantalla.

Figura 5-2 LAN

La siguiente tabla describe los campos de esta pantalla.

Tabla 5-1 LAN

ETIQUETA	DESCRIPCIÓN
DHCP	
DHCP	Si se configura a Server (servidor), su Prestige puede asignar direcciones IP, puerta enlace predeterminada y servidores DNS a cualquier cliente con soporte de cliente DHCP. Si se configura a **None** (No), el servidor DHCP estará deshabilitado. Si se configura como **Relay**, el Prestige actúa como un sustituto del servidor DHCP de manera que trapasa las peticiones y respuestas DHCP entre el servidor remoto y los clientes. Introduzca la dirección IP del servidor DHCP remoto en el campo **Remote DHCP Server** en este caso. Cuando se utilice DHCP, los siguientes puntos tendrán que se completados.
Client IP Pool Starting Address	Este campo especifica la primera de las direcciones IP contenidas en el pool.
Size of Client IP Pool	Este campo especifica el tamaño del pool de direcciones IP.
Primary DNS Server	Introduzca las direcciones IP de los servidores DNS. Estas direcciones son enviadas a los clientes DHCP junto con la dirección IP y la máscara de subred.
Secondary DNS Server	Igual a lo indicado arriba.
Remote DHCP Server	Si se selecciona el modo Relay en el campo DHCP entonces habrá que introducir aquí la dirección IP del servidor DHCP remoto.
TCP/IP	
IP Address	Introduzca la dirección IP de su Prestige en formato decimal, por ejemplo, 192.168.1.1 (por defecto).
IP Subnet Mask	Introduzca la máscara de subred asignada.
RIP Direction	Seleccione la dirección de los paquetes RIP entre None**, Both, In Only** y **Out Only.**
RIP Version	Seleccione la versión de RIP entre **RIP-1, RIP-2B** y **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) es un protocolo de red utilizado para establecer pertenencias en un grupo multicast. El Prestige soporta tanto la versión 1 como la 2 de IGMP (**IGMP-v1** e **IGMP-v2**). Seleccione **None** para deshabilitarlo.

Apply	Pulse **Apply** para guardar los cambios en el Prestige.
Cancel	Pulse **Cancel** para comenzar a configurar esta pantalla de nuevo.

Capítulo 6
Configuración de la LAN Inalámbrica

Este capítulo muestra como configurar los parámetros de la interfaz inalámbrica del Prestige.

6.1 Descripción de la LAN Inalámbrica

Esta sección introduce la interfaz LAN inalámbrica y algunas configuraciones básicas. Una red inalámbrica puede ser tan sencilla como un par de ordenadores con clientes inalámbricos comunicándose en modo peer-to-peer o tan compleja como un conjunto de ordenadores con clientes inalámbricos comunicándose a través de puntos de acceso que puentean el tráfico hacia la red LAN cableada.

Las pantallas WLAN sólo aparecerán cuando exista una tarjeta WLAN instalada

6.1.1 Requisitos de Instalación Adicionales para utilizar 802.1x

- Un ordenador con una tarjeta wireless LAN IEEE 802.11b/g y con un navegador web (con JavaScript habilitado) y/o Telnet.
- Una estación cliente inalámbrica debe estar ejecutando un software compatible 802.1x. Actualmente, Windows XP ofrece un cliente de este tipo.
- Un servidor RADIUS opcional para autenticación y contabilidad remota de usuarios.

6.1.2 Canal

Un canal es la frecuencia radio utilizada por los dispositivos wireless IEEE802.11b/g. Los canales disponibles dependerá de la región geográfica. Dentro de la posibilidad de elección de canales (para su zona) deberá utilizar canales diferentes para puntos de acceso adyacentes para reducir interferencias. Las interferencias aparecen cuando las señales radio procedentes de diferentes puntos de acceso se superponen provocando una degradación de la comunicación.

Sin embargo, los canales adyacentes se superponen parcialmente. Para evitar estas interferencias debidas al solapamiento, su punto de acceso deberá estar en un canal alejado al menos cinco canales del canal utilizado por otro punto de acceso adyacente. Por ejemplo, si su zona admite 11 canales y un punto de acceso adyacente está utilizando el canal 1, entonces necesitará seleccionar un canal entre el 6 y el 11.

6.1.3 EES ID

Un ESS (Extended Service Set) es un grupo de puntos de acceso o gateways wireless conectados a una red cableada en la misma subred. Un EES ID es un identificador único para cada dominio. Todos los puntos de acceso o gateways wireless y sus estaciones wireless asociadas dentro del dominio tienen el mismo ESSID.

6.1.4 RTS/CTS

El problema del nodo oculto ocurre cuando dos estaciones están dentro del rango del mismo punto de acceso, pero no están dentro del rango de cada uno de ellos, es decir, cada uno de las estaciones está fuera del rango de la otra. La siguiente figura muestra el problema del nodo oculto. Ambas estaciones (STA) están dentro del rango del AP, sin embargo, ellas no pueden “escucharse” entre sí. Cuando una estación empieza a transmitir datos con el punto de acceso, podría no saber que la otra estación está ya utilizando el medio wireless. De manera que son estaciones ocultas entre ellas.

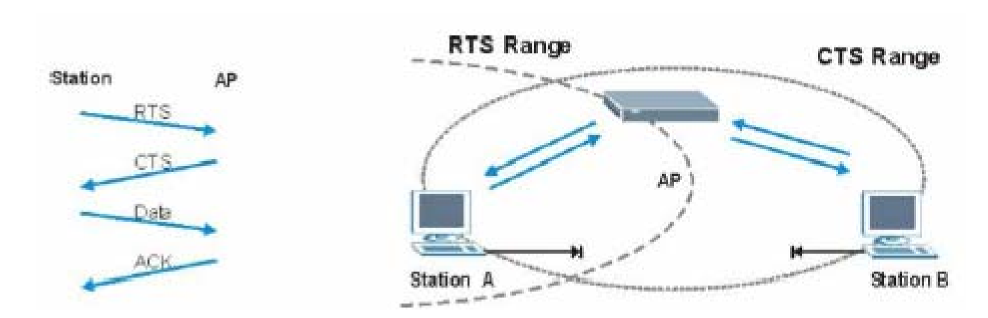


Figura 6-1 RTS/CTS

Cuando la estación A envía datos al Prestige, puede no saber que la estación B ya está utilizando el canal. Si estas dos estaciones envían datos al mismo tiempo, habrá colisión cuando ambos mensajes lleguen simultáneamente al punto de acceso. La colisión tendrá como resultado la pérdida de los mensajes de las dos estaciones.

RTS/CTS está diseñado para prevenir las colisiones debidas a los nodos ocultos. Un **RTS/CTS** define el tamaño máximo de paquete que se puede enviar antes de invocar un establecimiento RTS (Request to Send) / CTS (Clear to Send).

Cuando un paquete de datos excede el valor **RTS/CTS** configurado (entre 0 y 2432 bytes), la estación que desea transmitir ese paquete debe en primer lugar, envíar un mensaje RTS al punto de acceso pidiendo permiso para enviarlo. El punto de acceso responde con un mensaje CTS a todas las estaciones dentro de su rango notificándoles que detengan sus transmisiones. Esto igualmente reserva y confirma a la estación que ha llevado a cabo la petición el periodo de tiempo para la transmisión requerida.

Las estaciones pueden enviar paquetes de menor tamaño que el especificado por el valor **RTS/CTS** directamente al punto de acceso sin el establecimiento **RTS/CTS**.

Si el valor de **RTS/CTS** es mayor que el valor del **Umbral de Fragmentación** (**Fragmentation Threshold**), entonces el establecimiento **RTS/CTS** nunca se llevará a cabo puesto que los paquetes siempre serán fragmentados antes de alcanzar el tamaño **RTS/CTS**.

El habilitar el umbral RTS (RTS Threshold) introduce una redundancia en red que podría afectar negativamente a la tasa de transferencia en lugar de resultar beneficioso.

6.1.5 Umbral de Fragmentación (Fragmentation Threshold)

El **Umbral de Fragmentación (Fragmentation Threshold)** es el tamaño máximo del paquete (entre 256 y 2432 bytes) que puede ser transmitido a través de la red wireless antes de que el Prestige fragmente el paquete en trozos más pequeños.

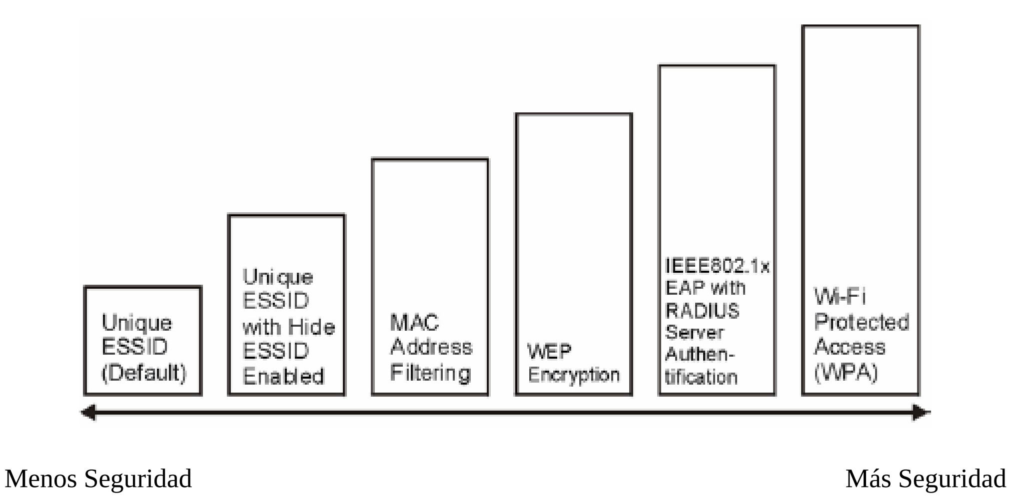
Se recomienda una valor alto para este umbral para redes no propensas a interferencias mientras que este valor deberá ser más pequeño para una red más saturada o redes propensas a las interferencias.

Si el valor del **Umbral de Fragmentación (Fragementation Threshold)** es más pequeño que el valor **RTS/CTS** configurado para el establecimiento **RTS/CTS**, entonces éste nunca se llevará a cabo puesto que los paquetes serán fragmentados antes de alcanzar el tamaño **RTS/CTS**.

6.2 Niveles de Seguridad

La seguridad en un entorno wireless es vital para proteger la comunicación wireless entre estaciones inalámbricas, puntos de acceso y red cableada.

La figura siguiente muestra los niveles de seguridad disponibles en su Prestige. EAP (Extensible Authentication Protocol) es utilizado para autenticación y utiliza intercambio de clave WEP dinámica. Requiere la interacción con un servidor RADIUS (Remote Authentication Dial-In User Service) bien en la WAN o en la LAN para proporcionar servicio de autenticación para las estaciones inalámbricas.



Menos Seguridad Más Seguridad

Figura 6-2 Niveles de Seguridad Wireless

Si no habilita ningún nivel de seguridad wireless en su Prestige, su red será accesible para cualquier dispositivo wireless dentro de esa área de cobertura.

Utilice el configurador web del Prestige para configurar los parámetros de seguridad de la wireless LAN. Consulte el capítulo sobre el uso del configurador web del Prestige para ver como acceder al configurador web.

6.3 Encriptación de datos y WEP

La encriptación WEP securiza los datos a transmitir entre las estaciones inalámbricas y los puntos de acceso para mantener la privacidad de las comunicaciones. Encripta tanto las comunicaciones unicast como multicast de la red. Tanto las estaciones wireless como los puntos de acceso utilizan la misma clave WEP para la encriptación y desencriptación de datos.

Su Prestige permite configurar hasta cuatro claves de 64-bits, 128-bits ó 256-bits aunque sólo una de ellas puede ser habilitada simultáneamente.

Para configurar y habilitar la encriptación WEP, pulse sobre **Wireless LAN** y **Wireless** para mostrar la pantalla **Wireless**.

6.4 Configurando la Wireless LAN

Si está configurando el Prestige desde un ordenador conectado a la interfaz wireless LAN y modifica los parámetros de EESI o WEP, perderá la conexión wireless cuando pulse Apply para guardar los cambios. Deberá cambiar los parámetros wireless en su ordenador de manera que coincidan con los nuevos configurados en el Prestige.

Pulse sobre **Wireless LAN, Wireless** para abrir la pantalla **Wireless**.

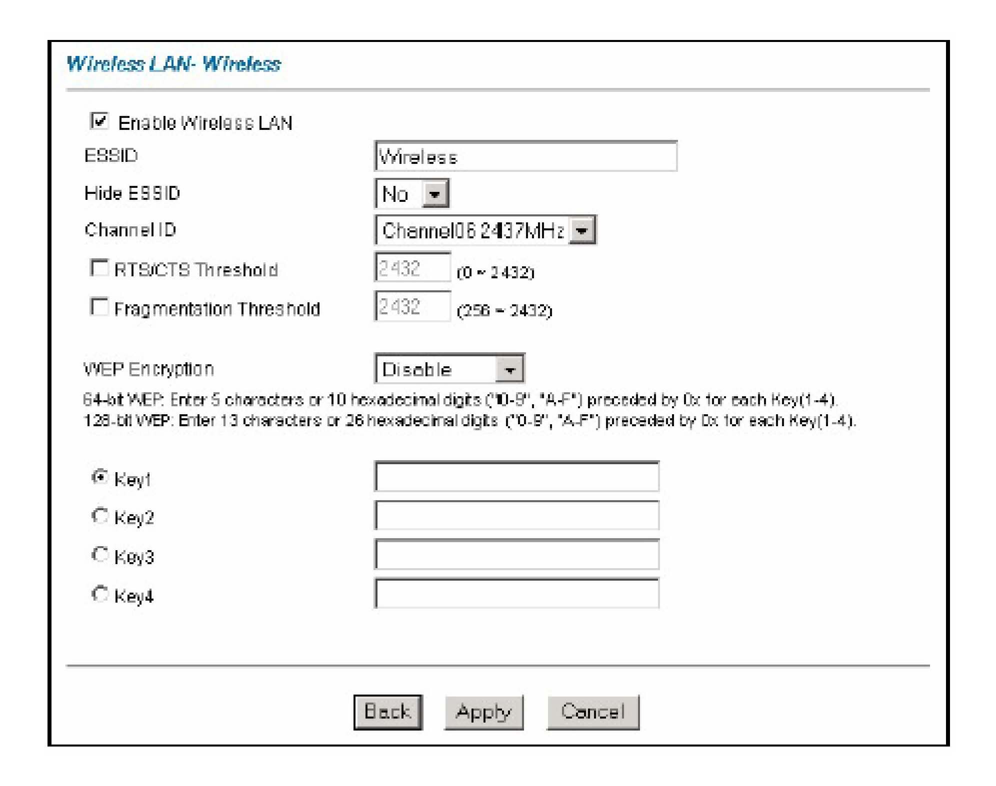


Figura 6-3 Wireless

La siguiente tabla describe los campos de esta pantalla.

Tabla 6-1 Wireless

ETIQUETA	DESCRIPCIÓN
Enable Wireless LAN	Utilice esta casilla para habilitar o deshabilitar la interfaz inalámbrica.
ESSID	El ESSID (Extended Service Set IDentifier) es un único nombre para identificar al Prestige en una red wireless. Los clientes wireless asociados a un punto de acceso tienen que tener el mismo ESSID. Introduzca un nombre descriptivo (hasta 32 caracteres).
Hide ESSID	Seleccione **Yes** para ocultar el ESSID de manera que una estación no pueda obtener el valor del ESSID mediante un escaneo pasivo.

	Seleccione **No** para hace el ESSID visible de manera que una estación pueda detectarlo mediante un escaneo pasivo.
Channel ID	La frecuencia radio utilizada por los dispositivos wireless 802.11b/g es llamada canal. Seleccione un canal de la lista desplegable.
RTS/CTS Threshold	El umbral RTS(Request To Send) (número de bytes) para habilitar la comunicación mediante RTS/CTS. Los datos con el tamaño de trama mayor que este valor, implementarán la comunicación RTS/CTS. Configurando este atributo para que sea mayor que el tamaño máximo del MSDU (Unidad de Datos de Servicio MAC) se elimanará la opción de que se produzca la comunicación RTS/CTS. Introduzca un valor entre 0 y 2432.
Fragmentation Threshold	El umbral (número de bytes) para la fragmentación de mensajes. Es el tamaño máximo de datos fragmentados que se pueden enviar. Introduzca un valor entre 256 y 2432
WEP Encryption	WEP (Wired Equivalent Privacy) encripta los paquetes de datos antes de transmitirlos por la red inalámbrica. Seleccione **Disable** para permitir que los dispositivos wireless se comuniquen con los puntos de acceso sin encriptación. Seleccione **64-bit WEP, 128-bit WEP** o **256-bit WEP** para utilizar encriptación de datos.
Key 1 to Key 4	Las claves WEP se utlizan para encriptar los datos. Tanto el Prestige como los clientes inalámbricos tienen que usar las mismas claves WEP para la transmisión de datos. Si selecciona **64-bit WEP**, introduzca 5 caracteres ASCII o 10 caracteres hexadecimales (“0-9”,”A-F”). Si selecciona **128-bit WEP**, introduzca 13 caracteres ASCII o 26 caracteres hexadecimales (“0-9”,”A-F”). Si selecciona **64-bit WEP**, introduzca 29 caracteres ASCII o 58 caracteres hexadecimales (“0-9”,”A-F”). Será necesario configurar las cuatro claves, aunque sólo una de ellas podrá ser utilizada a la vez. La clave por defecto es la clave 1.

Back	Pulse **Back** para volver a la pantalla principal de configuración Wireless LAN
Apply	Pulse **Apply** para guardar los cambios en el Prestige.
Cancel	Pulse **Cancel** para comenzar de nuevo.

6.5 Configuración del Filtrado MAC

La pantalla del filtrado MAC permite configurar el Prestige para permitir el acceso hasta a 32 dispositivos (Permitir Asociación – Allow Association) o excluir hasta a 32 dispositivos del acceso al Prestige (Denegar Asociación – Deny Association). Cada dispositivo Ethernet tiene una única dirección MAC. La dirección MAC es asignada en fábrica y consiste en seis pares de caracteres hexadecimales, por ejemplo, 00:A0:C5:00:00:02. Necesita conocer la dirección MAC de sus dispositivos para configurar esta pantalla.

Para cambiar los parámetros del filtrado MAC en su Prestige, pulse **Wireless LAN, MAC Filter** para abrir la pantalla del filtrado MAC (**MAC Filter**). La pantalla que aparece es.

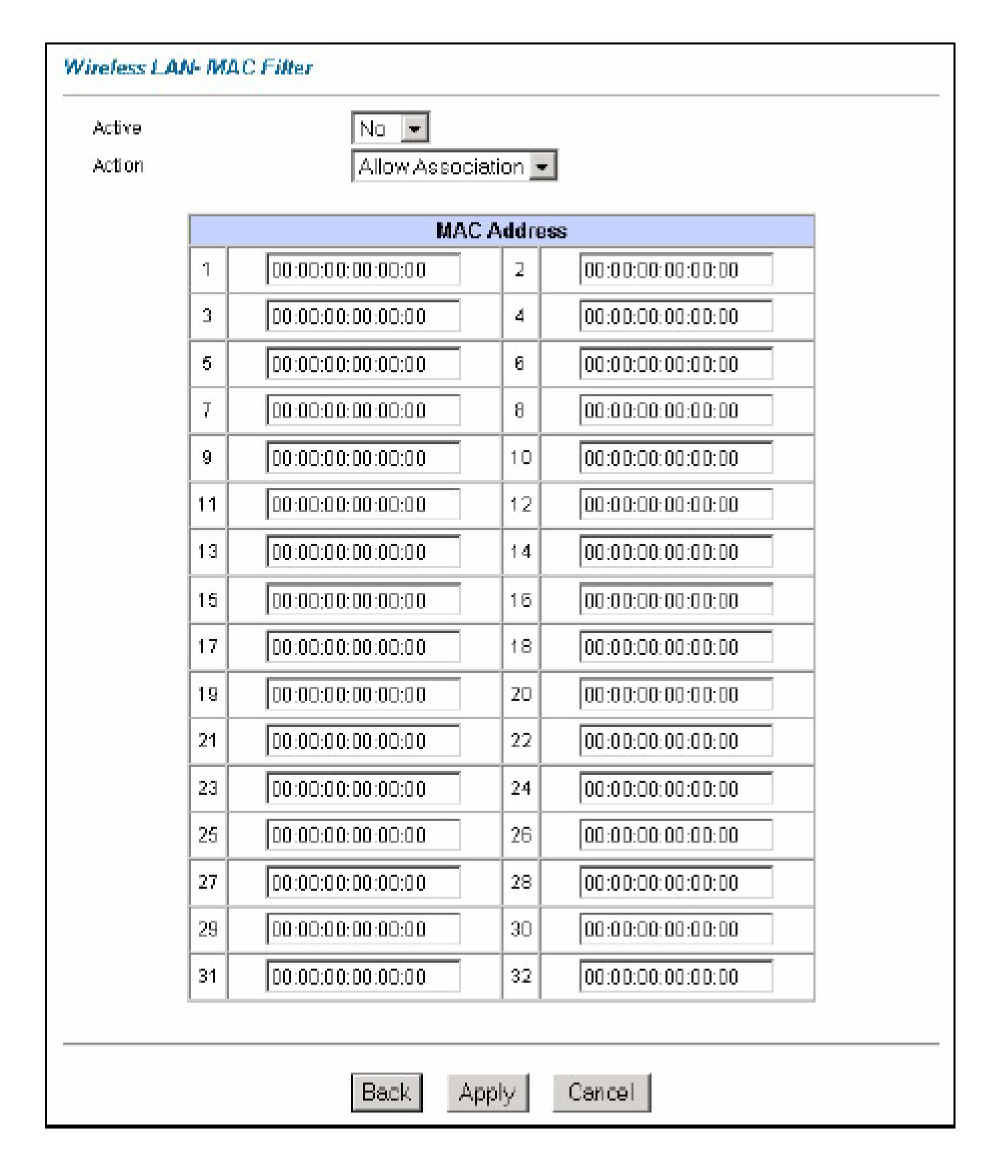


Figura 6-4 Filtrado por direcciones MAC

La siguiente tabla describe los campos de este menú.

ETIQUETA	DESCRIPCIÓN
Active	Seleccione **Yes** de la lista desplegable para habilitar el filtrado por direcciones MAC.
Action	Definir la acción de filtrado para las direcciones MAC contenidas en la lista. Seleccione **Deny Association** para bloquear el acceso al router, las direcciones MAC no contenidas en la lista podrán acceder al router. Seleccione **Allow Association** para permitir el acceso al router, las direcciones MAC no contenidas en la lista no se les permitirá el acceso al router.
MAC Address	Introduzca las direcciones MAC (en formato xx:xx:xx:xx:xx:xx) de la estación wireless a la que se permite o se deniega el acceso al Prestige.
Back	Pulse **Back** para volver a la pantalla principal wireless LAN.
Apply	Pulse **Apply** para guardar los cambios.
Cancel	Pulse **Cancel** para comenzar a configurar esta pantalla de nuevo.

6.6 Autenticación de Red

Puede configurar su Prestige y su red para autenticar una estación inalámbrica antes de que la estación wireless pueda comunicarse con el Prestige y la red cableada a la que el Prestige está conectada.

6.6.1 EAP

EAP es un protocolo de autenticación diseñado originalmente para ejecutarse sobre frames PPP (Protocolo Punto-a-Punto) para soportar múltiples tipos de autenticación de usuarios. El utilizar EAP para interactuar con un servidor RADIUS compatible con EAP, el punto de acceso ayuda en el proceso de autenticación mutua entre la estación wireless y el servidor RADIUS.

6.6.2 RADIUS

RADIUS está basado en un modelo cliente-servidor que soporta autenticación, autorización y contabilidad. El punto de acceso es el cliente y el servidor es el RADIUS. El servidor RADIUS lleva las siguientes tareas:

- **Autenticación**

Determina la identidad de los usuarios.

- **Autorización**

  Determina los servicios disponibles para los usuarios autenticados una vez que están conectados a la red.

- **Contabilidad**

  Lleva el control de la actividad de red de los clientes.

RADIUS consiste en un simple intercabmio de paquetes en el que el Prestige actúa como un intermediario de mensajes entre la estación inalámbrica y el servidor RADIUS.

Tipos de Mensajes RADIUS

Los siguientes tipos de mensajes RADIUS son intercambiados entre el punto de acceso y el servidor RADIUS para la autenticación de usuarios:

- **Access-Request**

  Enviado por un punto de acceso solicitando autenticación.

- **Access-Reject**

  Enviado por un servidor RADIUS rechazando el acceso.

- **Access-Accept**

  Enviado por un servidor RADIUS permitiendo el acceso.

- **Access-Challenge**

  Enviado por un servidor RADIUS solicitando más información para permitir el acceso. El punto de acceso envia una respuesta apropiada desde el usuario y después envia otro mensaje Access-Request.

Los siguientes tipos de mensajes RADIUS son intercambiados entre el punto de acceso y el servidor RADIUS para la contabilidad de usuarios:

- **Accounting-Request**

  Enviado por el punto de acceso solicitando contabilidad.

- **Accounting-Response**

  Enviado por el servidor RADIUS que ha comenzado o detenido la contabilidad.

Para asegurar la seguridad de la red, el punto de acceso y el servidor RADIUS utlizando un clave compartida, una contraseña, conocida por ambos. la información de contraseña es intercambiada de forma encriptada para proteger la red de accesos no autorizados.

6.6.3 Descripción Autenticación EAP

EAP (Extensible Authentication Protocol – Protocolo de Autenticación Extensible) es un protocolo de autenticación que se ejecuta en lo alto del mecanismo de transporte IEEE802.1x para soportar múltiples tipos de autenticación de usuario. El utilizar EAP para interactuar con un servidor RADIUS compatible con EAP, el punto de acceso ayuda en el proceso de autenticación mutua entre la estación wireless y el servidor RADIUS.

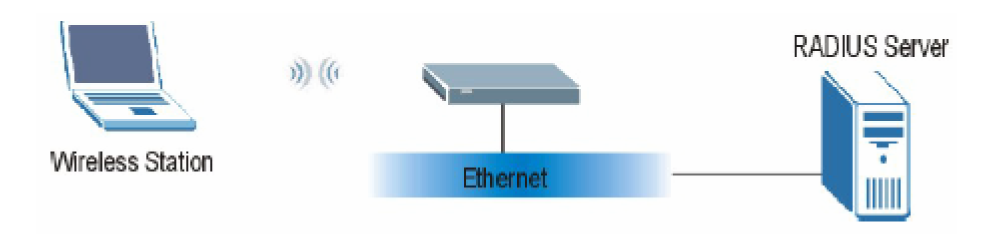


Figura 6-5 Autenticación EAP

Los siguientes detalles muestran una descripción general acerca del funcionamiento de la autenticación IEEE802.1x. Para un ejemplo sobre los pasos de autenticación EAP-MD5, consulte el apéndice sobre IEEE802.1x.

Paso 1.- La estación wireless envía un mensaje “inicio” al Prestige.

Paso 2.- El Prestige envía un mensaje de “petición de identidad” a la estación wireless.

Paso 3.- La estación wireless responde con la información requerida, incluyendo nombre de usuario y contraseña.

Paso 4.- El servidor RADIUS comprueba la información de usuario frente a su base de datos de perfiles de usuario y determina si autentica o no a la estación inalámbrica.

6.7 Introducción al WPA

Wi-Fi Protected Access (WPA) es un subconjunto de la especificación de seguridad IEEE802.11i. Las principales diferencias entre WPA y WEP son la autenticación de usuario y la mejora en la encriptación de datos.

6.7.1 Autenticación de Usuario

WPA aplica IEEE802.1x y el protocol EAP en la autenticación de los clientes inalámbricos utilizando una base de datos RADIUS externa. No es posible utilizar la Base de Datos local del Prestige para autenticación WPA dado que la Base de Datos Local utiliza EAP-MD5 la cuál no puede ser utilizada para la generación de claves. Vea más adelante en este capítulo y en los apéndices más información acerca de IEEE802.1x, RADIUS y EAP.

De todas formas, si no dispone de un servidor RADIUS externo debería utilizar WPA-PSK (WPA Pre-Shared Key) que únicamente requiere que se especifique una password (idéntica) en cada punto de acceso, gateway wireless y cliente wireless. Si el password coincide, el cliente podrá acceder a la Wireless LAN.

6.7.2 Encriptación

WPA mejora la encriptación de datos utilizando Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) y IEEE802.1x.

TKIP utiliza claves de 128 bits que son dinámicamente generadas y distribuidas por el servidor de autenticación. Incluye una función de mezcla de clave por paquete, un Comprobador de la Integridad del Mensaje (MIC – Message Integrity Check), un vector de inicialización (IV) con reglas secuenciales y un mecanismo de re-codificación.

TKIP cambia y rota regularmente las claves de encriptación de manera que la misma clave de encriptación no se utiliza nunca dos veces. El servidor RADIUS distribuye una clave PMK (Pairwise Master Key) al AP que establece una jerarquía de claves y un sistema de gestión, utilizando la clave PMK para generar dinámicamente claves de encriptación de datos únicas para encriptar cada paquete de datos que es comunicado por el medio inalámbrico entre el punto de acceso y los clientes wireless. Esto se ejecuta en el background automáticamente.

El MIC (Comprobación de la Integridad del Mensaje) está diseñado para prevenir que un alguien pueda capturar los paquetes de datos, alterarlos y reenviarlos. El MIC proporciona una fuerte función matemática que calculan tanto el receptor como el transmisor y a posteriori comparan el valor del MIC. Si no coinciden, se asume que los datos han sido interceptados y el paquete se tira.

Generando claves de encriptación únicas para cada paquete de datos y creando un mecanismo de verificación de la integridad (MIC), TKIP hace mucho más complicado que WEP el decodificar los datos en una red Wi-Fi, haciendo muy difícil el que un intruso pueda acceder a los contenidos transmitidos por la red.

Los mecanismos de encriptación utilizados para WPA y WPA-PSK son los mismos. La única diferencia entre ellos es que WPA-PSK utiliza una simple contraseña, en lugar de los datos específicos del usuario. La utilización de la password en WPA-PSK hace que ésta sea susceptible de ataques aunque todavía supone una gran mejora sobre la encriptación WEP.

6.8 Ejemplo de Aplicación WPA-PSK

Una aplicación con WPA-PSK sería:

Paso 1.- En primer lugar introduzca passwords idénticas en el punto de acceso y los clientes wireless. La PSK debe contener entre 8 y 63 caracteres ASCII.

Paso 2.- El punto de acceso chequea la password del cliente y (únicamente) permite que se una a la red si existe coincidencia de contraseña.

Paso 3.- El punto de acceso distribuye claves a los clientes wireless.

Paso 4.- El punto de acceso y los clientes wireless utilizan el proceso de encriptación TKIP para encriptar los datos intercambiados entre ellos.

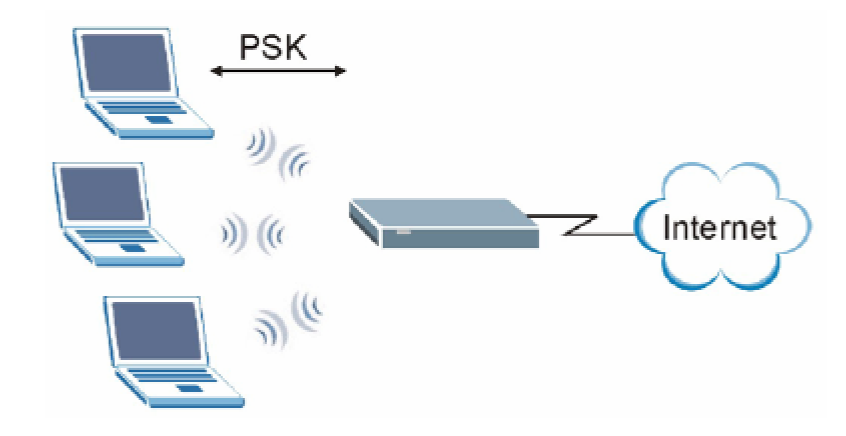


Figura 6-6 Autenticación WPA

6.9 Ejemplo de Aplicación de WPA con RADIUS

Necesita la dirección IP de un servidor RADIUS, el número de puerto (por defecto 1812) y la contraseña compartida con el RADIUS. Un ejemplo de aplicación WPA con un servidor RADIUS externo se muestra como sigue. "A" es el servidor RADIUS. "DS" es el sistema de distribución.

Paso 1.- El punto de acceso pasa la petición de autenticación del cliente wireless al servidor RADIUS.

Paso 2.- El servidor RADIUS chequea la identificación del usuario frente a su base de datos y permite o deniega el acceso a red.

Paso 3.- El servidor RADIUS distribuye la clave PMK (Pairwise Master Key) al punto de acceso que genera una jerarquía de claves y un sistema de gestión, utilizando la PMK para generar dinámicamente claves de encriptación únicas para encriptar los paquetes de datos que sean intercambiados entre el punto de acceso y los clientes wireless por el medio radio.

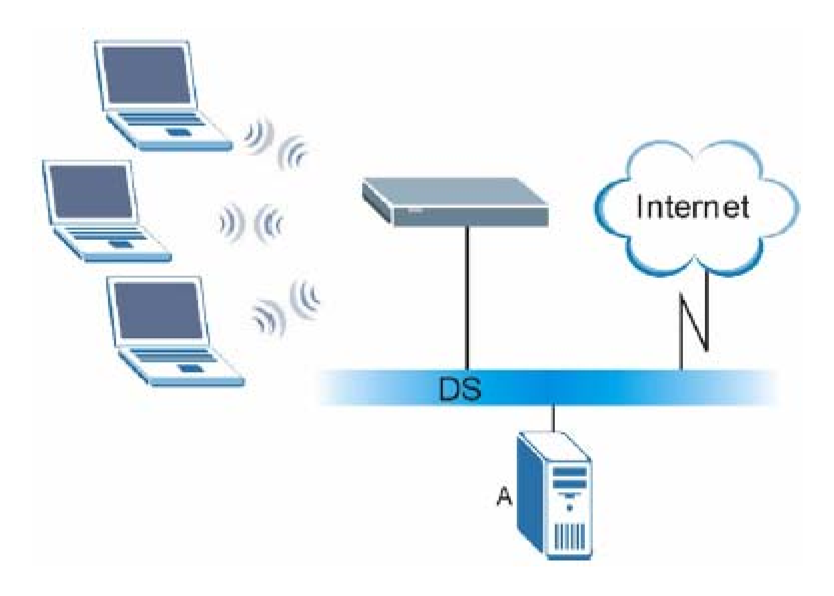


Figura 6-7 Ejemplo de Aplicación WPA con RADIUS

6.10 Resumen de Parámetros de Seguridad

Consulte esta tabla para ver qué otros parámetros de seguridad debe configurar para cada Método de Autenticación/tipo de protocolo de gestión de claves. Las claves se introducen seleccionando en primer lugar 64-bit WEP ó 128-bit WEP en el campo WEP Encryption y después tecleando las claves (en formato ASCII o Hexadecimal). Los filtros de direcciones MAC no dependen de cómo se configuren estas reglas de seguridad.

Tabla 6-3 Matriz Parámetros de Seguridad Wireless

MÉTODO DE AUTENTICACIÓN/ PROTOCOLO DE GESTIÓN DE CLAVES	**MÉTODO DE ENCRIPTACIÓN**	**ENTRADA DE CLAVE MANUAL**	**IEEE802.1X HABILITADO**
Abierto (Open)	Ninguno	No	No
Abierto (Open)	WEP	No	Habilitado con clave WEP dinámica

		Sí	Habilitado sin clave WEP dinámica
		Sí	Deshabilitado
Compartido (Shared)	WEP	No	Habilitado con clave WEP dinámica
		Sí	Habilitado sin clave WEP dinámica
		Sí	Deshabilitado
WPA	WEP	No	Sí
WPA	TKIP	No	Sí
WPA-PSK	WEP	Sí	Sí
WPA-PSK	TKIP	Sí	Sí

6.11 Clientes Wireless WPA

Un cliente wireless WPA es un software que se ejecuta en un sistema operativo para instruir al cliente wireless sobre como utilizar WPA. En el momento de escribir, los clientes más desarrollados son el parche WPA para Windows XP, cliente Odyssey de Funk Software y el cliente AEGIS de Meetinghouse Data Communications.

El parche de Windows XP es un software gratis que permite añadir capacidades WPA al cliente wireless de Windows XP. Sin embargo, es necesario utilizar Windows XP para disponer del mismo.

6.12 Configurando 802.1x y WPA

Para modificar los parámetros de autenticación de su Prestige, pulse sobre el enlace **Wireless LAN** bajo **Advanced Setup** y después en la pestaña **802.1x/WPA**. La pantalla varía en función del protocolo de gestión de claves que se seleccione.

La siguiente pantalla aparece cuando selecciona **No Access Allowed** o **No Authentication Required** en el campo **Wireless Port Control**.

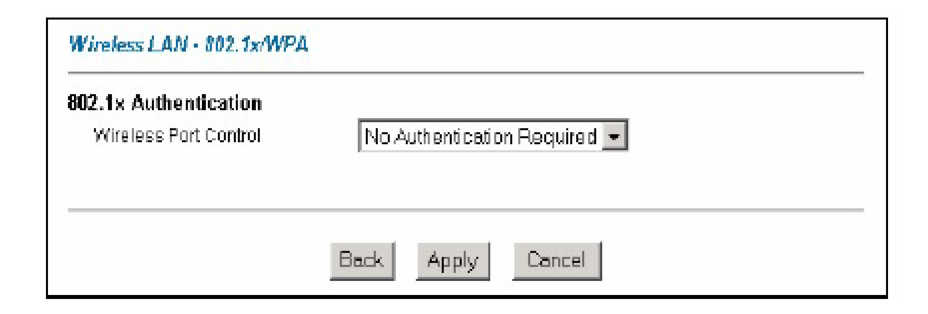


Figura 6-8 Wireless LAN : 802.1x/WPA

La siguiente tabla describe los campos de esta pantalla.

Tabla 6-4 Wireless LAN : 802.1x/WPA

ETIQUETA	DESCRIPCIÓN
Wireless Port Control	Para controlar el acceso de las estaciones wireless a la red cableada, seleccione un método de control de la lista desplegable. Elija entre **No Access Allowed, No Authentication Required** y **Authentication Required**. **No Access Allowed** bloquea el acceso de todas las estaciones wireless. **No Authentication Required** permite el acceso de todas las estaciones wireless a la red cableada sin introducir ni nombre de usuario de usuario ni contraseña. Configuración por defecto. **Authentication Required** indica que las estaciones wireless tienen que introducir nombre de usuario y contraseña antes de acceder a la red cableada. Seleccione **Authentication Required** para configurar el protocolo de gestión de claves (**Key Management Protocol)** y otros campos relativos.
Back	Pulse **Back** para volver a la pantalla principal de Wireless LAN.
Apply	Pulse **Apply** para guardar los cambios.
Cancel	Pulse **Cancel** para comenzar la configuración de esta pantalla de nuevo.

Authentication Required : 802.1x (Autenticación Requerida : 802.1x)

Seleccione **Authentication Required** en el campo **Wireless Port Control** y **802.1x** en el campo **Key Management Protocol** para mostrar la siguiente pantalla.

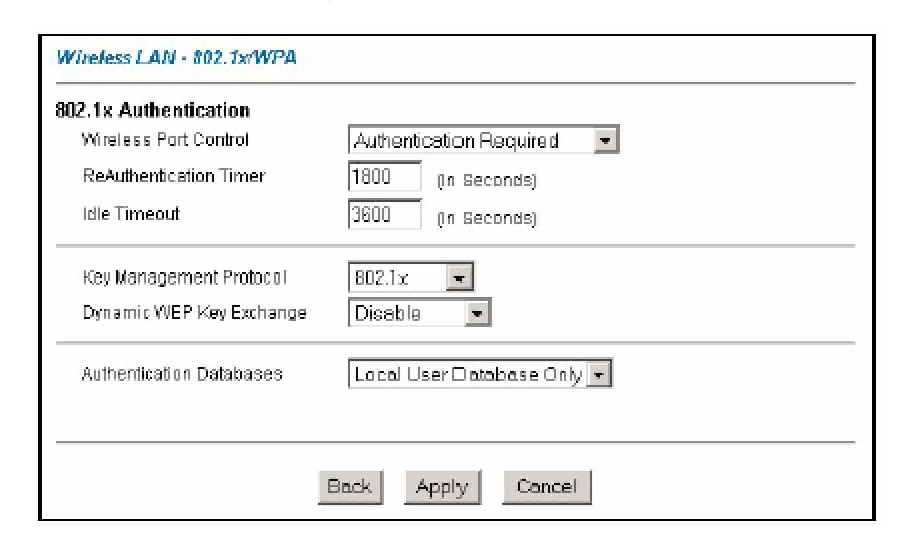


Figura 6-9 Wireless LAN : 802.1x/WPA con protocolo 802.1x

La siguiente tabla describe las etiquetas en esta pantalla.

Tabla 6-5 Wireless LAN : 802.1x/WPA con protocolo 802.1x

ETIQUETA	DESCRIPCIÓN
Wireless Port Control	Para controlar el acceso de las estaciones wireless a la red cableada, seleccione un método de control de la lista desplegable. Elija entre **No Access Allowed, No Authentication Required** y **Authentication Required**. Los siguientes campos sólo están disponibles cuando selecciona **Authentication Required**.
ReAuthentication Timer (en segundos)	Especifique cada cuanto tiempo tienen las estaciones wireless que reintroducir el nombre de usuario y contraseña para seguir conectadas. Este campo está activado únicamente cuando se selecciona **Authentication Required** en el campo **Wireless Port Control**. Introduzca el intervalo de tiempo entre 10 y 9999 segundos. El intervalo por defecto es de **1800** segundos (30 minutos).

	Si la autenticación de la estación wireless se lleva a cabo utilizando un servidor RADIUS, el temporizador de reautenticación del RADIUS tendrá la prioridad.
Idle Timeout (en segundos)	El Prestige automáticamente desconecta una estación wireless de la red cableada tras un periodo de inactividad. La estación wireless necesita introducir nuevamente el usuario y la contraseña antes de volver a acceder a la red cableada. Este campo está activado sólo cuando se selecciona **Authentication Required** en el campo **Wireless Port Control**. El valor por defecto es de **3600** segundos (ó 1 hora).
Key Management Protocol	Seleccione **802.1x** en la lista desplegable.
Dynamic WEP Key Exchange	Este campo está activado sólo cuando se selecciona **Authentication Required** en el campo **Wireless Port Control**. Y el campo **Authentication Databases** configurado a **RADIUS Only**. Seleccione **Disable** para permitir que las estaciones wireless se comuniquen con los puntos de acceso sin utilizar intercambio de clave WEP dinámica. Seleccione **64-bit WEP** ó **128-bit WEP** para habilitar la encriptación de datos. Hasta 32 estaciones pueden acceder al Prestige cuando se configura el intercambio de clave WEP dinámica. Este campo no estará disponible cuando se seleccione **Key Management Protocol** como **WPA** o **WPA-PSK**.
Authentication Databases	La base de datos de autenticación contiene información de acceso de la estación wireless. La base de datos local es la base de datos incluida en el Prestige. El RADIUS es un servidor externo. Utilice la lista desplegable para seleccionar qué base de datos debe utilizar el Prestige (en primer lugar) para autenticar a las estaciones inalámbricas. Antes de especificar la prioridad, asegúrese que tiene correctamente configuradas las correspondientes bases de datos. Seleccione **Local User Database Only** para que el Prestige únicamente chequee en la base de datos del Prestige el nombre de usuario y contraseña de una estación wireless. Seleccione **RADIUS Only** para que el Prestige únicamente chequee en la base de datos en un servidor RADIUS específico el nombre de usuario y contraseña de una estación wireless. Seleccione **Local first, then RADIUS** para que el Prestige chequee en primer lugar la

	base de datos local en el Prestige el nombre de usuario y contraseña de la estación wireless. Si el nombre de usuario no se encuentra, el Prestige comprobará el usuario en la base de datos del servidor RADIUS especificado. Seleccione **RADIUS first, then Local** para que el Prestige chequee en primer lugar en la base de datos del servidor RADIUS el nombre de usuario y contraseña de la estación wireless. Si el Prestige no puede conectar con el servidor RADIUS, entonces chequeará la base de datos local del Prestige. Cuando el nombre de usuario no se encuentra o la password no coincide en el servidor RADIUS, el Prestige no chequeará la base de datos local y la autenticación fallará.
Back	Pulse **Back** para volver a la pantalla principal del menú Wireless LAN.
Apply	Pulse **Apply** para guardar los cambios.
Cancel	Pulse **Cancel** para comenzar a configurar esta pantalla de nuevo.

Una vez habilite la autenticación de usuario, tendrá que especificar un servidor RADIUS externo o crear cuentas de usuario en la base de datos local del Prestige para autenticación.

Authentication Required : WPA (Autenticación Requerida : WPA)

Seleccione Authentication Required en el campo Wireless Port Control y WPA y en el campo Key Management Protocol para mostrar la siguiente pantalla.

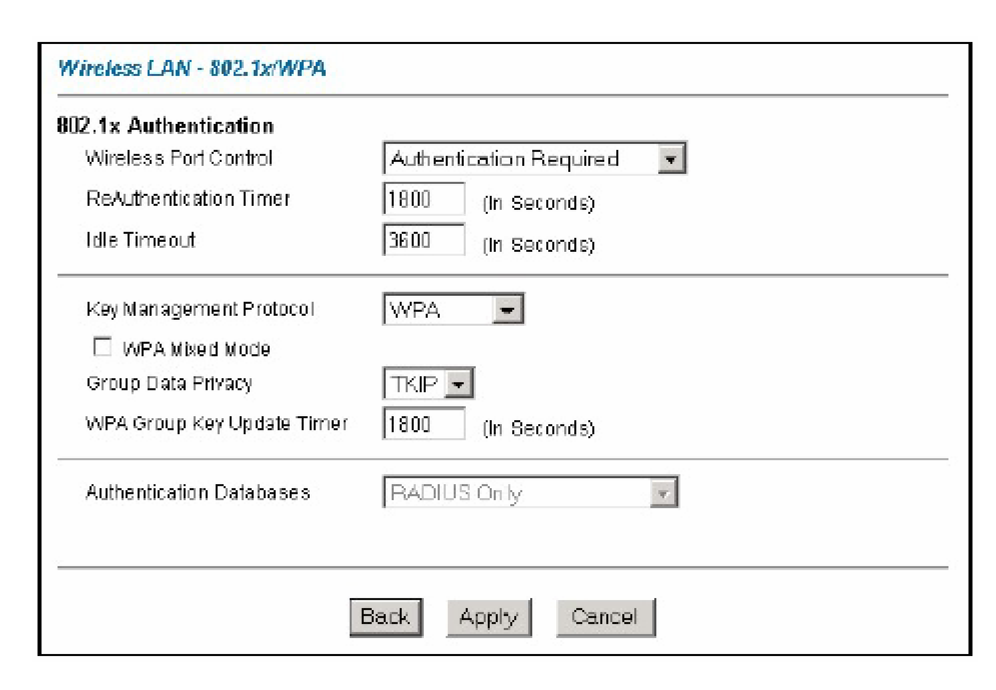


Figura 6-10 Wireless LAN : 802.1x/WPA con Protocolo WPA

La siguiente tabla describe las etiquetas que no se han visto con anterioridad.

Tabla 6-6 Wireless LAN : 802.1x/WPA con Protocolo WPA

ETIQUETA	DESCRIPCIÓN
Key Management Protocol	Seleccione **WPA** en este campo.
WPA Mixed Mode	El Prestige puede operar en **WPA Mixed Mode**, el cuál soporta clientes tanto con WPA como clientes con intercambio de WEP dinámica con 802.1x en la misma red Wi-Fi. Seleccione la casilla para activar el modo WPA mezclado. De otra forma, no seleccione la casilla y configure el campo **Group Data Privacy**.
Group Data Privacy	**Group Data Privacy** permite seleccionar **TKIP** (recomendado) o **WEP** para tráfico broadcast y multicast si el **Key Management Protocol** es **WPA** y el **WPA Mixed Mode** está deshabilitado. El **WEP** se utiliza automáticamente si se habilita el **WPA Mixed Mode**.

	Todo el tráfico unicast es automáticamente encriptado por **TKIP** cuando se configura **WPA** o **WPA-PSK**.
WPA Group Key Update Timer	El **WPA Group Key Timer** es el periodo en el que el punto de acceso (si está utilizando **WPA-PSK**) o el servidor RADIUS (si se utiliza **WPA**) envía un nuevo grupo de claves a los clientes. El proceso de renovación de claves es en WPA el equivalente a cambiar la clave WEP para un AP y las estaciones wireless en una wireless LAN. La configuración del **WPA Group Key Update Timer** también se soporta en el modo WPA-PSK. El valor por defecto es de 1800 segundos (30 minutos).
Authentication Databases	Cuando se configura el **Key Management Protocol** como **WPA**, el valor de **Authentication Databases** debe ser **RADIUS Only**. Sólo se podrá utilizar la base de datos local (**Local User Database Only**) con el protocolo **802.1x**.

Authentication Required : WPA-PSK (Autenticación Requerida : WPA-PSK)

Seleccione **Authentication Required** en el campo **Wireless Port Control** y **WPA-PSK** en el campo **Key Management Protocol** para mostrar la siguiente pantalla.

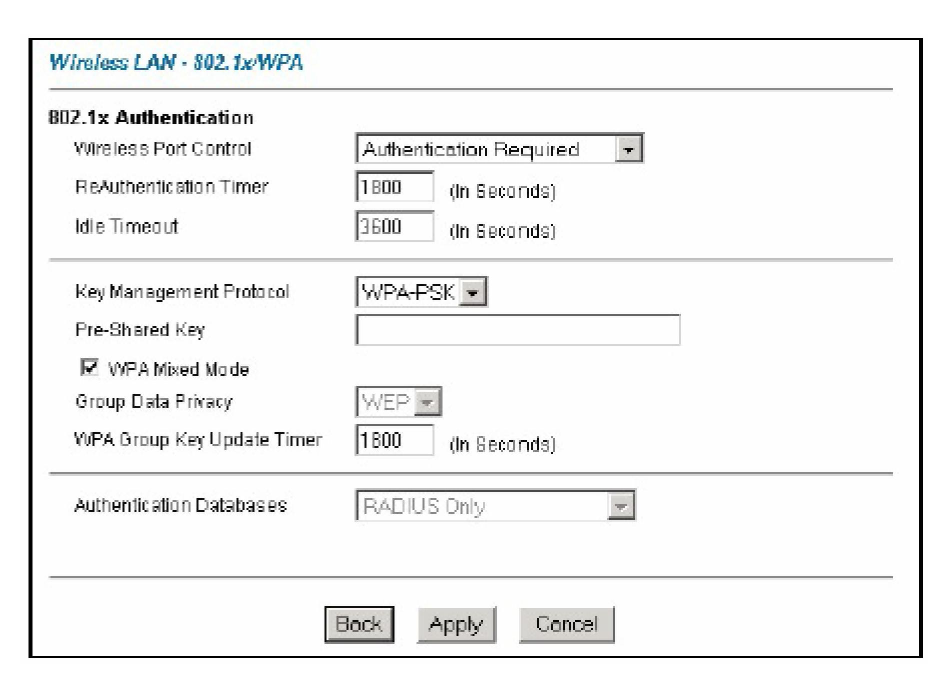


Figura 6-11 Wireless LAN : 802.1x/WPA con Protocolo WPA-PSK

La siguiente tabla describe las etiquetas no mencionadas anteriormente.

Tabla 6-7 Wireless LAN : 802.1x/WPA con Protocolo WPA-PSK

ETIQUETA	DESCRIPCIÓN
Key Management Protocol	Seleccione **WPA-PSK**.
Pre-Shared Key	El mecanismo de encriptación utilizado por **WPA** y **WPA-PSK** es el mismo. La única diferencia entre ellos es que **WPA-PSK** utiliza una contraseña en lugar de credenciales específicas de usuario. Introduzca una clave entre 8 y 63 caracteres ASCII.
WPA Mixed Mode	El Prestige puede operar en **WPA Mixed Mode**, que soporta tanto clientes WPA como clientes con intercambio dinámico de WEP con 802.1x en la misma red Wi-Fi. Seleccione la casilla para activar el modo WPA

	mezclado. De otra forma, desmarque la casilla y configure el campo **Group Data Privacy**.
Group Data Privacy	**Group Data Privacy** permite seleccionar entre **TKIP** (recomendado) o **WEP** para el tráfico broadcast y multicast si el **Key Management Protocol** es **WPA** y **WPA Mixed Mode** está deshabilitado. **WEP** se utiliza automáticamente si se habilita **WPA Mixed Mode**. Todo el tráfico unicast es encriptado automáticamente mediante **TKIP** cuando se selecciona **WPA** o **WPA-PSK**.
Authentication Databases	Este campo únicamente estará visible cuando el modo **WPA Mixed** esté habilitado.

6.13 Configurando la Autenticación de Usuarios Local

Almacenando los perfiles de usuarios de forma local, el Prestige es capaz de autenticar a los usuarios wireless sin necesidad de un servidor RADIUS externo. Sin embargo, existe un límite en el número de usuarios que pueden autenticarse de esta manera.

Para modificar la base de datos local del Prestige, pulse **Wireless LAN, Local User Database**. La pantalla que aparece es:

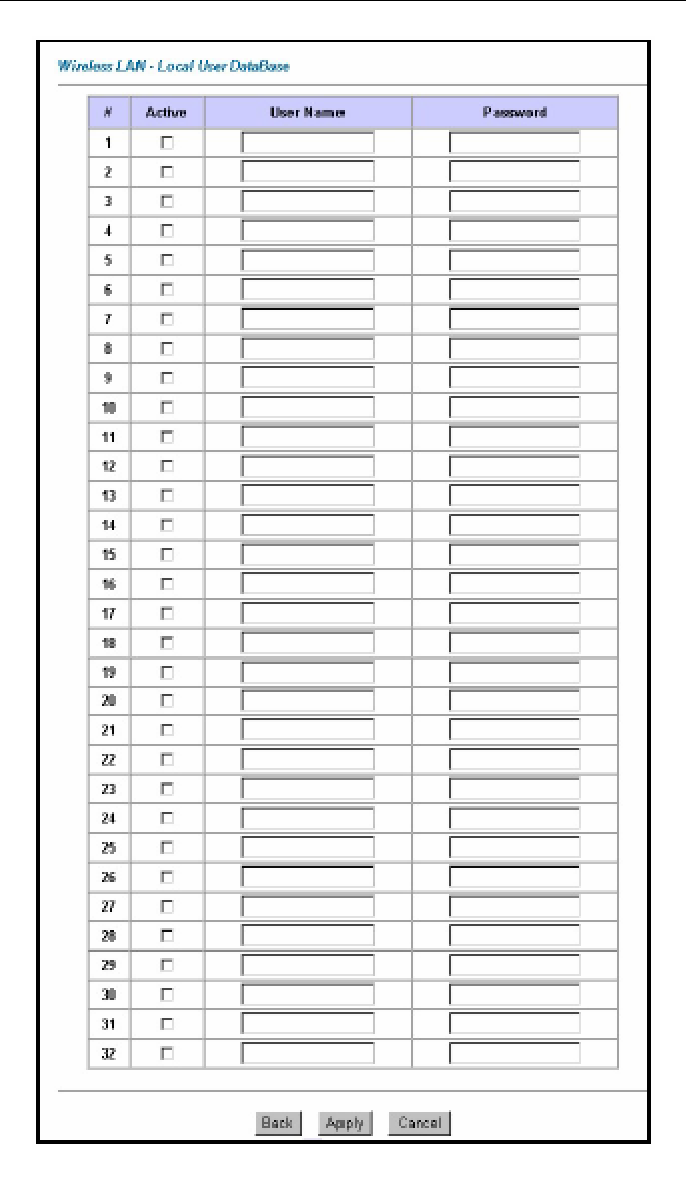


Figura 6-12 Base de Datos Local

La siguiente tabla describe los campos de esta pantalla.

Tabla 6-8 Base de Datos Local

ETIQUETA	DESCRIPCIÓN
#	Éste es el índice de la cuenta de usuario local.
Active	Seleccione esta casilla para habilitar este perfil.
User Name	Introduzca el nombre de usuario para este perfil.
Password	Introduzca la password de hasta 31 caracteres para este perfil.
Back	Pulse Back para volver a la pantalla principal Wireless LAN.
Apply	Pulse Apply para guardar los cambios.
Cancel	Pulse Cancel para volver a configurar esta pantalla de nuevo.

6.14 Configurando el RADIUS

Una vez que se habilita al autenticación EAP, es necesario especificar un servidor externo para la autenticación y la contabilidad de los usuarios remotos.

Para configurar los parámetros del servidor RADIUS en el Prestige, pulse **Wireless LAN, RADIUS**. La pantalla que aparece es la siguiente.

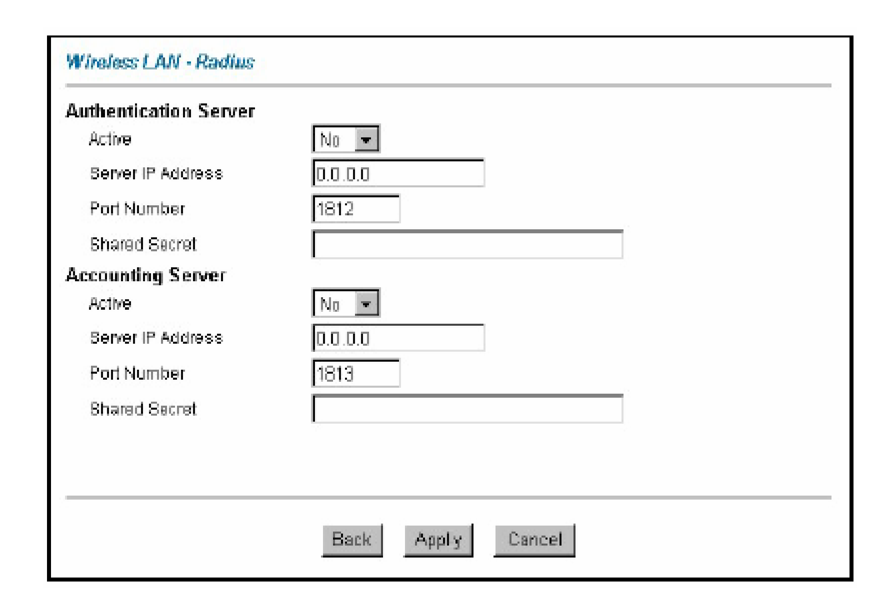


Figura 6-13 RADIUS

La siguiente tabla describe los campos de esta pantalla.

Tabla 6-9 RADIUS

ETIQUETA	DESCRIPCIÓN
Authentication Server	
Active	Seleccione **Yes** de la lista desplegable para habilitar la autenticación de usuarios a través de un servidor externo de autenticación.
Server IP Address	Introduzca la dirección IP del servidor externo de autenticación en formato decimal.
Port Number	El puerto por defecto del servidor RADIUS para la autenticación es **1812**.
Shared Secret	Introduzca la password (de hasta 31 caracteres) como la clave compartida entre el servidor RADIUS y los puntos de acceso. La clave no es enviada a través de la red. Esta clave

	tiene que ser la misma en el servidor externo y en el Prestige.
Accounting Server	
Active	Seleccione **Yes** de la lista desplegable para habilitar la contabilidad de usuarios a través de un servidor externo de contabilidad.
Server IP Address	Introduzca la dirección IP del servidor externo de contabilidad en formato decimal.
Port Number	El puerto por defecto del servidor RADIUS para la contabilidad es **1813**.
Shared Secret	Introduzca la password (de hasta 31 caracteres) como la clave compartida entre el servidor RADIUS y los puntos de acceso. La clave no es enviada a través de la red. La clave tiene que ser la misma en el servidor externo y en los puntos de acceso.
Back	Pulse **Back** para volver a la pantalla principal Wireless LAN.
Apply	Pulse **Apply** para guardar los cambios.
Cancel	Pulse **Cancel** para volver a configurar esta pantalla de nuevo.

Capítulo 7
Configuración WAN

Este capítulo versa describe como configurar los parámetros WAN.

7.1 Descripción WAN

Una red de área global (WAN) es una conexión exterior hacia otra red en Internet. Consulte el capítulo del Asistente de Configuración para más información sobre los campos de las pantallas WAN.

7.2 Métrica

La métrica representa el "coste de transmisión". Un router determina la mejor ruta para una transmisión eligiendo el caminio con el menor "coste". El protocolo de routing RIP utiliza el número de saltos como una medida del coste, con un valor mínimo de "1" para redes conectadas directamente. El número deberá estar entre "1" y "15", un número mayor de "15" indicará que el enlace está caído. Cuanto menor sea el número, menor será el "coste".

La métrica indica la prioridad de las rutas del Prestige hacia Internet. Si existen cualquier par de rutas con la misma métrica, el Prestige utiliza las siguientes prioridades predefinidas:

1. Ruta normal : Diseñada por el ISP (consultar sección 7.5)
2. Ruta para redirección del tráfico (consultar sección 7.6)

Por ejemplo, si la ruta normal tiene métrica "1" y la ruta para la redirección de tráfico tiene métrica "2", entonces la ruta normal actúa como la ruta por defecto primaria. Si la ruta normal falla en su conexión con Internet, el Prestige intenta la siguiente ruta definida para la redirección del tráfico.

Las Políticas de Routing IP tienen prioridad sobre las rutas mencionadas anteriormente (consulte el capítulo sobre Políticas de Routing IP)

7.3 Encapsulación PPPoE

El Prestige soporta PPPoE (Point-to-Point Protocol over Ethernet). PPPoE es un estándar del IETF (RFC 2516) que especifica como un ordenador personal (PC) interactúa con un módem de banda ancha (DSL, cable, wireless, etc.). La opción PPPoE se utilizará para conexiones dial-up PPPoE.

Para el proveedor de servicio, PPPoE ofrece un método de acceso y autenticación que funciona con sistemas de control de acceso existentes (por ejemplo RADIUS). PPPoE proporciona un login y un método de autenticación que el software de Microsoft Dial-UP Networking puede activar, y que adicionalmente no requiere nuevos conocimientos o procedimientos para usuarios Windows.

Uno de los beneficios de PPPoE es la habilidad para permitir el acceso a uno de los múltiples servicios de red, una función conocida como selección dinámica de servicio. Esto posibilita al proveedor del servicio el crear y ofrecer de forma sencilla nuevos servicios para determinados usuarios.

De forma operativa, PPPoE ahorra esfuerzos significativamente tanto para el usuario como para el ISP, dado que no require una configuración específica en el módem de banda ancha en el lado del cliente.

Implementando PPPoE directamente en el Prestige (en lugar de en los ordenadores personales), los ordenadores en la LAN no necesitan un software PPPoE instalado, dado que el Prestige realiza esta tarea. Además, con NAT, todos los ordenadores de LAN podrán disfrutar del acceso.

7.4 Traffic Shaping

El Traffic Shaping se produce como un acuerdo entre el proveedor y el suscriptor para regular la tasa media y de pico o la fluctuación de la transmisión de datos sobre una red ATM. Este acuerdo ayuda a eliminar la congestión, lo cual es importante para la transmisión de datos en tiempo real en situaciones como transmisión de vídeo y audio.

Peak Cell Rate (PCR) es la tasa máxima a la cual el emisor puede enviar celdas. Este parámetro puede estar por debajo (pero no por encima) de la velocidad máxima de la línea. 1 celda ATM son 53 bytes (424 bits), así que una velocidad de línea de 832 Kbps da una PCR máxima de 1962 celdas/seg. Esta tasa no está garantizada porque depende de la velocidad de la línea.

Sustained Cell Rate (SCR) es la tasa de media de celdas que de cada fuente de tráfico en ráfagas. Especifica la tasa media máxima a la que se pueden enviar celdas por la conexión virtual. SCR no puede ser mayor que la PCR; por defecto es 0 celdas/seg.

Maximum Burst Size (MBS) es el número máximo de celdas que pueden ser enviadas a velocidad PCR. Cuando se alcanza la MBS, la tasa de celdas baja por debajo de la SCR hasta que la tasa media alcanza el valor SCR de nuevo. En ese momento, más celdas (hasta MBS) pueden ser enviadas a la tasa PCR.

Si los valores de PCR, SCR o MBS están por defecto a “0”, el sistema asignará un valor máximo adecuado

a la velocidad del upstream de la línea

La figura siguiente ilustra la relación entre PCR, SCR y MBS.

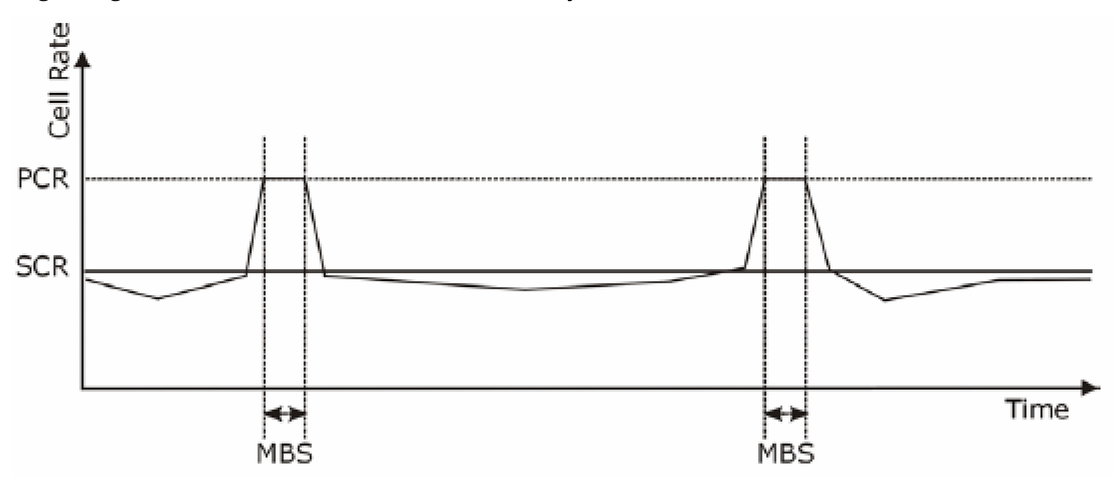


Figura 7-1 Ejemplo de Traffic Shaping

7.5 Configurando la interfaz WAN

Para modificar los parámetros de configuración del nodo remoto WAN del Prestige, pulse sobre **WAN, WAN Setup**. La pantalla se diferencian por la encapsulación.

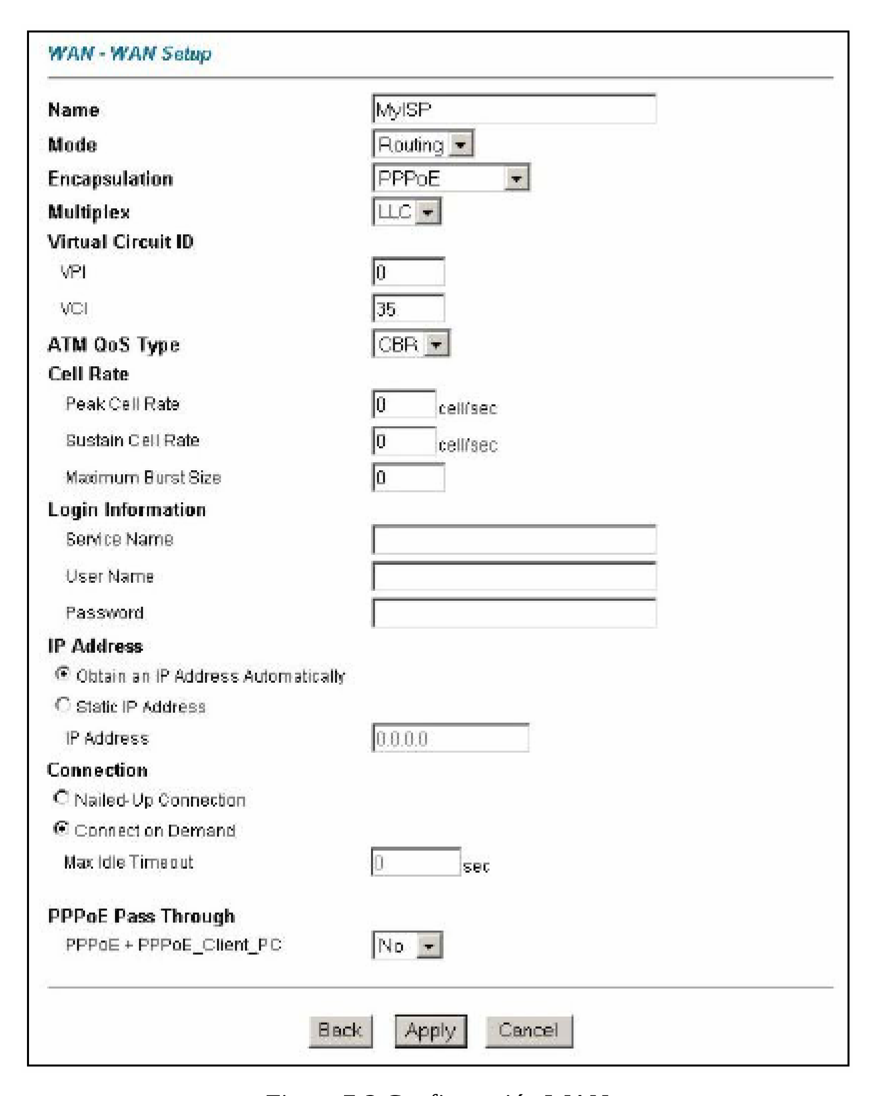


Figura 7-2 Configuración WAN

La siguiente tabla describe los campos de esta pantalla.

Tabla 7-1 Configuración WAN

ETIQUETA	DESCRIPCIÓN
Name	Introduzca el nombre de su Proveedor de Servicios de Internet, por ejemplo, MyISP. Estos datos son meramente identificativos.
Mode	Seleccione **Routing** (por defecto) de la lista desplegable si su ISP permite que múltiples ordenadores compartan el acceso a Internet. En cualquier otro caso, seleccione **Bridge**.
Encapsulation	Seleccione el método de encapsulación utilizado por su ISP de la lista desplegable. Las opciones dependerán del modo seleccionado en el campo **Mode**. Si selecciona **Bridge** en el campo **Mode**, escoja **PPPoA** o **RFC1483**. Si selecciona **Routing** en el campo **Mode**, seleccione entre **PPPoA, RFC1483, ENET ENCAP** o **PPPoE**.
Multiplex	Seleccione el método de multiplexación utilizado por su ISP de la lista desplegable. Las opciones son **VC** o **LLC**.
VPI	El rango válido para VPI es de 0 a 255. Introduzca el valor de VPI asignado.
VCI	El rango válido para VCI es de 32 a 65535 (del 0 al 31 están reservados para gestión local del tráfico ATM). Introduzca el valor del VCI asignado.
ATM QoS Type	Seleccione **CBR** (Continuos Bit Rate) para especificar un ancho de banda constante para el tráfico de voz o datos. Seleccione **UBR** (Unspecified Bit Rate) para aplicaciones que no son sensibles al tiempo, tales como el e-mail. Seleccione **VBR** (Variable Bit Rate) para tráfico en ráfagas y ancho de banda compartido con otras aplicaciones.
Cell Rate	La configuración de la tasa de celdas a menudo permite eliminar congestiones de tráfico que pueden ralentizar la transmisión de datos en tiempo real como las conexiones de audio y video.
Peak Cell Rate	Divide la tasa de la línea ADSL (bps) por 424 (el tamaño de una celda ATM) para calcular el valor del Peak Cell Rate (PCR). Ésta es la tasa máxima a la que el emisor puede enviar celdas. Introduzca aquí el valor de PCR.
Sustain Cell Rate	La Sustain Cell Rate (SCR) indica la tasa media de celdas (largo plazo) que pueden ser transmitidas. Introduzca el SCR, que debe ser inferior a la PCR. Por defecto, es 0 celdas/seg.
Maximum Burst Size	Maximum Burst Size (MBS) se refiere al número máximo de celdas que pueden ser enviadas a la tasa PCR. Introduzca el valor de MBS, que debe ser menor que 65535.

Login Information	(Sólo para encapsulaciones PPPoA o PPPoE)
Service Name	(Sólo PPPoE) Introduzca el nombre del servicio PPPoE
User Name	Introduzca el nombre de usuario tal y como se lo asigne su ISP.
Password	Introduzca la contraseña asociada con el nombre de usuario anterior.
IP Address	Esta opción esta disponible si selecciona **Routing** en el campo **Mode**. Una dirección IP estática es una dirección IP fija que le asigna su ISP. Una dirección IP dinámica no es fija; el ISP asigna una diferente cada vez que se conecta a Internet. La facilidad Single User Account puede ser utilizada tanto con dirección IP dinámica como estática. Seleccione **Obtain an IP Address Automatically** si tiene direccionamiento dinámico; en otro caso, seleccione **Static IP Address** y teclee la dirección IP asignada por su ISP en el campo **IP Address**.
Connection (Sólo encapsulación PPPoA y PPPoE).	La(s) regla(s) de llamada definidas en el menú 26 del SMT tendrán prioridad sobre los parámetros definidos en **Connection**.
Nailed-up Connection	Seleccione **Nailed-up Connection** cuando desea que su conexión esté siempre establecida. El Prestige intentará establecer la conexión siempre que la vea desconectada.
Connect on Demand	Seleccione **Connect on Demand** cuando no desee que la conexión esté siempre levantada y configure un temporizador en el campo **Max Idle Timeout**.
Max Idle Timeout	Especifique un temporizador de inactividad en el campo **Max Idle Timeout** cuando seleccione **Connect on Demand**. El valor por defeco es 0, lo que significa que la sesión de Internet nunca tendrá temporización de inactividad.
PPPoE Pass Through	Esta campo estará disponible cuando seleccione la encapsulación PPPoE.
PPPoE + PPPoE_Client_PC (sólo encapsulación PPPoE)	Adicionalmente al cliente PPPoE integrado en el Prestige, es posible habilitar el PPPoE pass through para permitir que hasta 10 usuarios en la LAN utilicen sus clientes software PPPoE en sus ordenadores para conectar con su ISP a través del Prestige. Cada host puede tener cuentas separadas y una dirección WAN IP pública. PPPoE pass through es una alternativa para el NAT para aplicaciones donde el NAT no es apropiado. Deshabilite el PPPoE pass through si no necesita habilitar que los hosts en la LAN utilicen software de cliente PPPoE en sus ordenadores para conectar con su ISP.

Subnet Mask (sólo encapsulación ENET ENCAP)	Introduzca la máscara de subred en formato decimal. Consulte el Apéndice Subnetting sobre como calcular la máscara de subred si está implementando subnetting.
ENET ENCAP Gateway (sólo encapsulación ENET ENCAP)	Debe especificar la dirección IP del gateway (proporcionada por el ISP) cuando seleccione **ENET ENCAP** en el campo **Encapsulation**.
Back	Pulse **Back** para volver a la pantalla anterior.
Apply	Pulse **Apply** para guardar los cambios.
Cancel	Pulse **Cancel** para comenzar a configurar esta pantalla de nuevo.

7.6 Redirección de Tráfico

La redirección de tráfico envía el tráfico a un gateway de backup cuando el Prestige no puede conectar con internet. Se muestra un ejemplo en la siguiente figura.

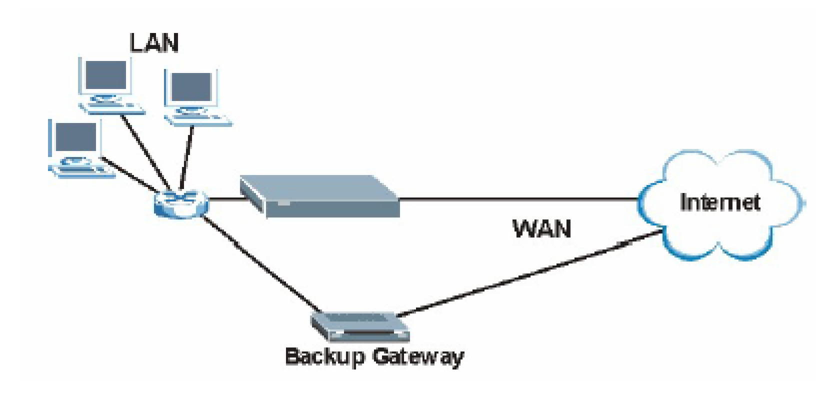


Figura 7-3 Ejemplo Redirección de Tráfico

La siguiente topología de red le permite evitar el problema de seguridad de la ruta del triángulo cuando el gateway de backup está conectado a la LAN. Utilice IP Alias para configurar la LAN con dos o tres redes lógicas con el Prestige como gateway para cada red LAN. Coloque la LAN protegida en una subred (Subred 1 en la siguiente figura) y el gateway de backup en otra subred (Subred 2). Configure filtros para permitir paquetes desde la LAN protegida (subred 1) al gateway de backup (subred 2).

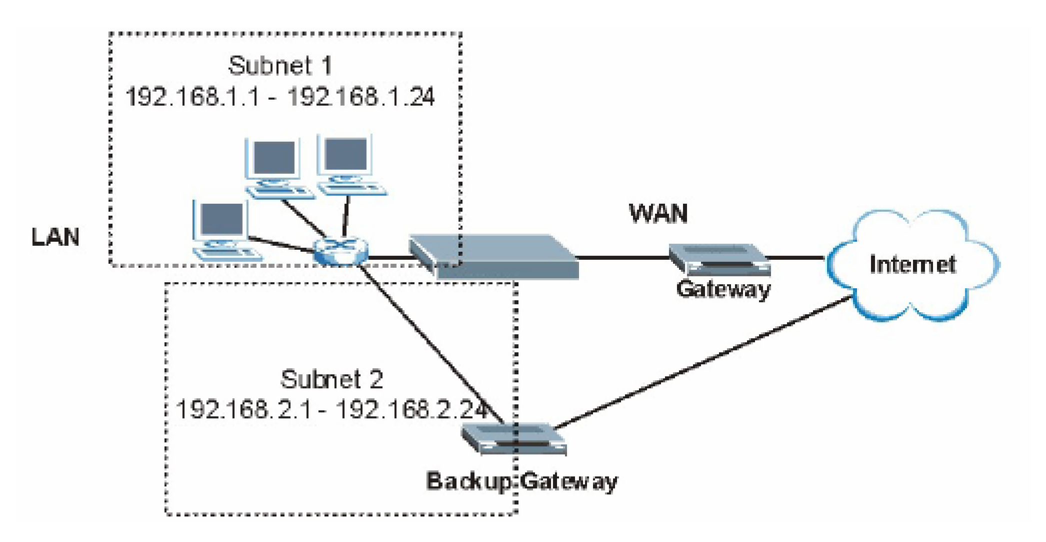


Figura 7-4 Redirección de Tráfico configurada en LAN

Capítulo 8
Network Address Traslation (NAT)

Este capítulo describe como configurar el NAT en el Prestige

8.1 Descripción NAT

NAT (Network Address Translation - NAT, RFC 1631 - Traslación de dirección de red) es la traslación de la dirección IP de una máquina en un paquete, por ejemplo, sería cambiar la dirección fuente de un paquete de salida, usada en una red a una dirección IP diferente conocida dentro de otra red.

8.1.1 Definiciones NAT

Interno / externo denota dónde está colocada la máquina respecto al Prestige, por ejemplo, los ordenadores de los usuarios están como máquinas internas, mientras que los servidores web en Internet son máquinas externas.

Global / local denota la dirección IP de una máquina en un paquete que pasa a través del router, por ejemplo, la dirección local se refiere a la dirección IP de una máquina cuando el paquete está en la red local, mientras que dirección global se refiere a la dirección IP de la máquina cuando el mismo paquete va por el lado WAN.

Resaltar que interior / exterior se refiere a la localización de una máquina, mientras global / local se refiere a la dirección IP que va en un paquete. Entonces, una dirección local interna (ILA) es la dirección IP de una máquina interna en un paquete cuando el paquete está todavía en la red local, mientras que dirección global interna (IGA) es la dirección IP de la misma máquina interna cuando el paquete está en el lado WAN. La siguiente tabla resume esta información.

Tabla 8-1 Definiciones NAT

TÉRMINO	DESCRIPCIÓN
Inside	Se refiere a una máquina en la LAN.
Outside	Se refiere a una máquina en la WAN.
Local	Se refiere a la dirección del paquete (origen o destino) con la que el paquete viaja en la LAN
Global	Se refiere a la dirección del paquete (origen o destino) con la que el paquete viaja en la

	WAN.

NAT nunca cambia la dirección IP (local o global) de una máquina externa.

8.1.2 Qué hace NAT

En la forma más simple, NAT cambia la dirección IP de la fuente en un paquete recibido de un usuario (la dirección local interna) a otra (la dirección global interna) antes de enviar el paquete al lado WAN. Cuando vuelve la respuesta, NAT traslada la dirección de destino (la dirección global interna) de nuevo a la dirección local interna antes de enviar el paquete a la máquina interna de origen. Tenga en cuenta que la dirección IP (local o global) de una máquina externa nunca se cambia.

Las direcciones IP globales para los hosts internos pueden ser asignadas o bien estática o bien dinámicamente por el ISP. Además, puede designar servidores, por ejemplo, un servidor web y un servidor telnet, en su red local y hacerlos accesibles al exterior. Si no define ningún servidor (para mapeo Many-to-One y Many-to-Many Overload – vea *Tabla 8-2*), NAT ofrece el beneficio adicional de la protección. Si no hay servidores definidos, el Prestige elimina filtrando todas las peticiones entrantes, evitando así que intrusos accedan a su red. Para más información de traducción de direcciones IP, consulte el *RFC 1631*, *The IP Network Address Translator (NAT)*.

8.1.3 Cómo funciona NAT

Cada paquete tiene dos direcciones – una dirección de origen y una dirección de destino. Para paquetes salientes, la ILA (dirección interna local) es la dirección origen de la LAN, y la IGA (dirección interna global) es la dirección origen de la WAN. Para paquetes entrantes, la ILA es la dirección de destino de la LAN, y la IGA es la dirección de destino de la WAN. NAT mapea las direcciones IP privadas (locales) IP a direcciones globales únicas requeridas para comunicarse con hosts de otras redes. Reemplaza la dirección IP de origen original (y los números de puerto de origen TCP o UDP mapeando Many-to-One y Many-to-Many Overload) en cada paquete y luego lo reenvía a Internet. El Prestige guarda un registro de las direcciones originales y de los números de puerto de forma que en los paquetes entrantes de respuesta se puedan establecer los valores originales. Esto se ilustra en la siguiente figura.

Figura 8-1 Cómo funciona NAT

8.1.4 Aplicación de NAT

La siguiente figura ilustra una posible aplicación de NAT, en la que tres LANs internas (LANs lógicas usando IP Alias) detrás del Prestige pueden comunicarse con tres redes WAN distintas. Puede ver más ejemplos al final de este capítulo.

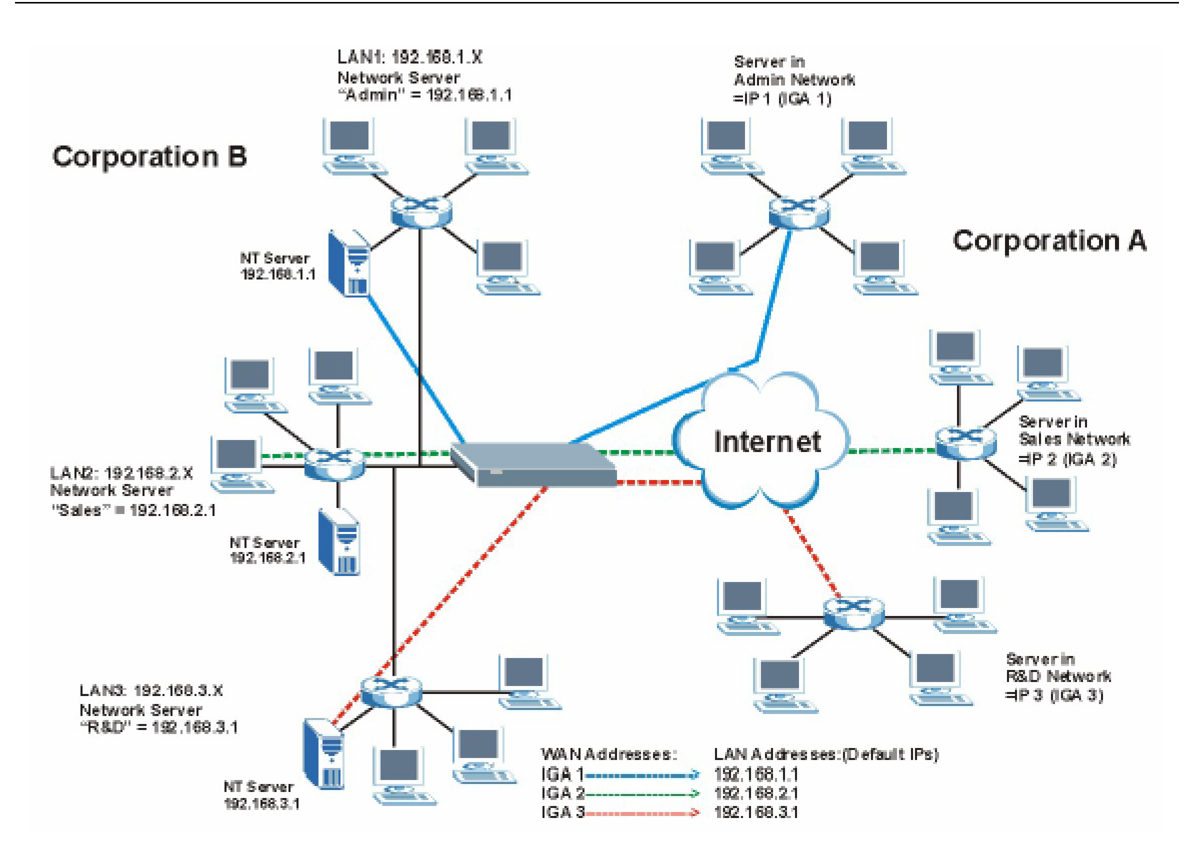


Figura 8-2 Aplicación NAT con IP Alias

8.1.5 Tipos de Mapeo NAT

NAT soporta cinco tipos de mapeo de IP / puerto. Estos son:

1. **One to One**: En este modo, el Prestige mapea una dirección IP local a una dirección IP global.
2. **Many to One**: En modo Many-to-One, el Prestige mapea múltiples direcciones IP locales a una dirección IP global. Es equivalente al SUA (por ejemplo, PAT, traducción de dirección de puerto), la característica Single User Account que soportaban los routers ZyXEL previos (la opción **SUA Only** en los routers actuales).
3. **Many to Many Overload**: En este modo, el Prestige mapea múltiples direcciones IP locales a direcciones IP globales compartidas.

4. **Many-to-Many No Overload**: En modo Many-to-Many No Overload, el Prestige mapea cada dirección IP local a una única dirección IP global.

5. **Server**: Este tipo le permite especificar servidores internos de diferentes servidores detrás del NAT para que puedan ser accesibles desde el exterior.

Los números de puerto no cambian para los tipos de mapeo NAT One-to-One **y** Many-to-Many No Overload**.**

La siguiente tabla resume estos tipos.

Tabla 8-2 Tipos de Mapeo NAT

TIPO	MAPEO IP	ABREVIATURA SMT
One-to-One	ILA1←→ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M:1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M:M Ov
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M:M No OV
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

8.2 SUA (Single User Account) frente a NAT

SUA (Single User Account) es una implementación ZyNOS de un subconjunto de NAT que soporta dos tipos de mapeo, **Many-to-One** y **Server**. El Prestige también soporta **Full Feature** NAT para mapear múltiples direcciones IP globales a múltiples direcciones IP de LAN privada de clientes o servidores usando tipos de mapeo como los descritos en la Tabla 8-2.

1. **Seleccione** SUA Only **si solamente tiene una dirección WAN IP pública para el Prestige.**

2. **Seleccione** Full Feature **si tiene múltiples direcciones WAN IP públicas para el Prestige.**

8.3 Servidor SUA

El conjunto de servidores SUA consiste en una lista de servidores internos (tras el NAT en la LAN), por ejemplo, web o FTP, que puede hacer visibles desde el exterior incluso aunque el SUA haga que toda su red aparezca en el exterior como un único equipo.

Podrá introducir un número de puerto individual o un rango de puertos, y la dirección IP local del servidor deseado. El número de puerto identifica el servicio; por ejemplo, el servicio web está en el puerto 80 y el FTP en el 21. En algunos casos, tales como para servicios desconocidos o donde un servidor puede soportar más de un servicio (por ejemplo, ambos servicios web y FTP), sería preferible especificar un rango de puertos. De esta manera puede asignar una dirección IP para un servidor que corresponda a un puerto o rango de puertos.

Dirección IP del servidor por defecto

Adicionalmente a los servidores para servicios específicos, NAT soporta la dirección IP de un servidor por defecto. El servidor por defecto recibe los paquetes para puertos no especificados en las reglas individuales.

Si no se asigna dirección IP en *Server Set 1* (servidor por defecto), el Prestige descarta todos los paquetes recibidos a los puertos que no están especificados aquí o en la configuración de gestión remota.

8.3.1 Reenvío de puertos : Servicios y Números de puerto

Los números de puerto usados más frecuentemente se muestran en la siguiente tabla. Por favor, consulte con la RFC1700 para más información sobre estos puertos.

Tabla 8-3 Servicios y Números de Puerto

SERVICIOS	NÚMERO DE PUERTO
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

8.3.2 Configuración de Servidores tras SUA (Ejemplo)

Supongamos que quiere asignar los puertos 21-25 a un servidor FTP, Telnet y SMTP (A en el ejemplo), el puerto 80 a otro (B en el ejemplo) y asignar el servidor por defecto a la dirección IP 192.168.1.35 (C en el ejemplo). Usted decidirá las direcciones IP de la LAN y el ISP asignará la dirección IP de la WAN. El NAT hace que la red aparezca como un simple ordenador en Internet.

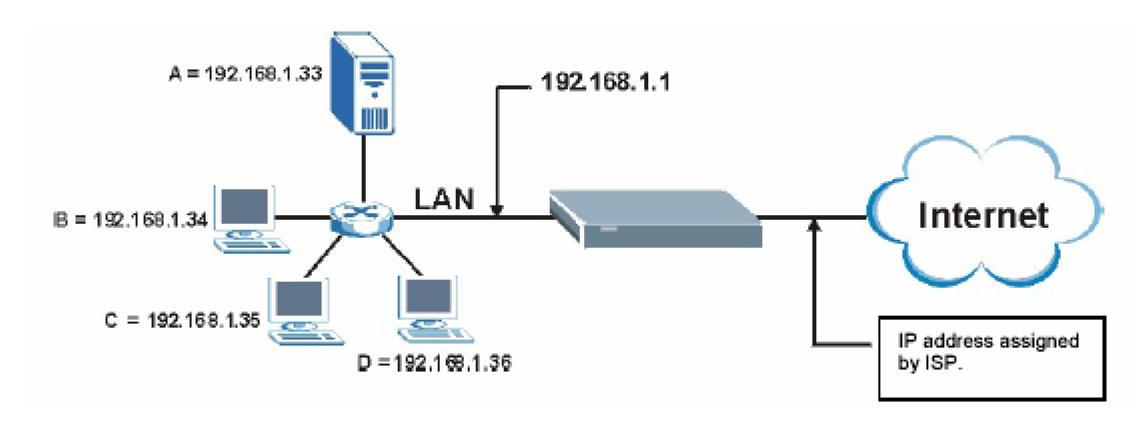


Figura 8-3 Ejemplo de Mútiples Servidores tras el NAT

8.4 Selección del modo NAT

Pulse sobre **NAT** para abrir la siguiente pantalla.

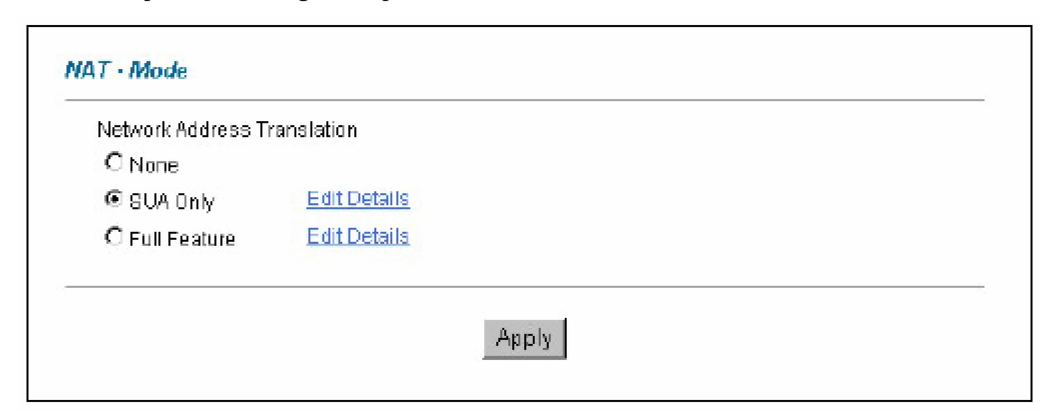


Figura 8-4 Modo NAT

La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 8-4 Modo NAT

ETIQUETA	DESCRIPCIÓN
None	Seleccione esta opción para deshabilitar el NAT
SUA Only	Seleccione esta opción si únicamente tiene una dirección pública en la WAN del Prestige. El Prestige utilizará el conjunto 1 para el mapeo de direcciones definido en la pantalla **NAT- Edit SUA/NAT Server Set**
Edit Details	Pulse este enlace para entrar en la pantalla **NAT – Edit SUA/NAT Server Set**
Full Feature	Seleccione esta opción si dispone de múltiples direcciones públicas en el interfaz WAN de su Prestige.
Edit Details	Pulse sobre este link para entrar en la pantalla **NAT - Address Mapping Rules**
Apply	Pulse sobre **Apply** para guardar la configuración

8.5 Configuración de SUA

Si no asigna ninguna dirección en el *Server Set 1* (default server – servidor por defecto), el Prestige descartará todos los paquetes recibidos para puertos que no estén especificados aquí o en la configuración de la gestión remota.

Pulse sobre **NAT**, seleccione **SUA Only** y a continuación sobre **Edit Details** para abrir la siguiente pantalla.

Consulte la Tabla 8-3 para ver los puertos usados más frecuentemente para servicios particulares.

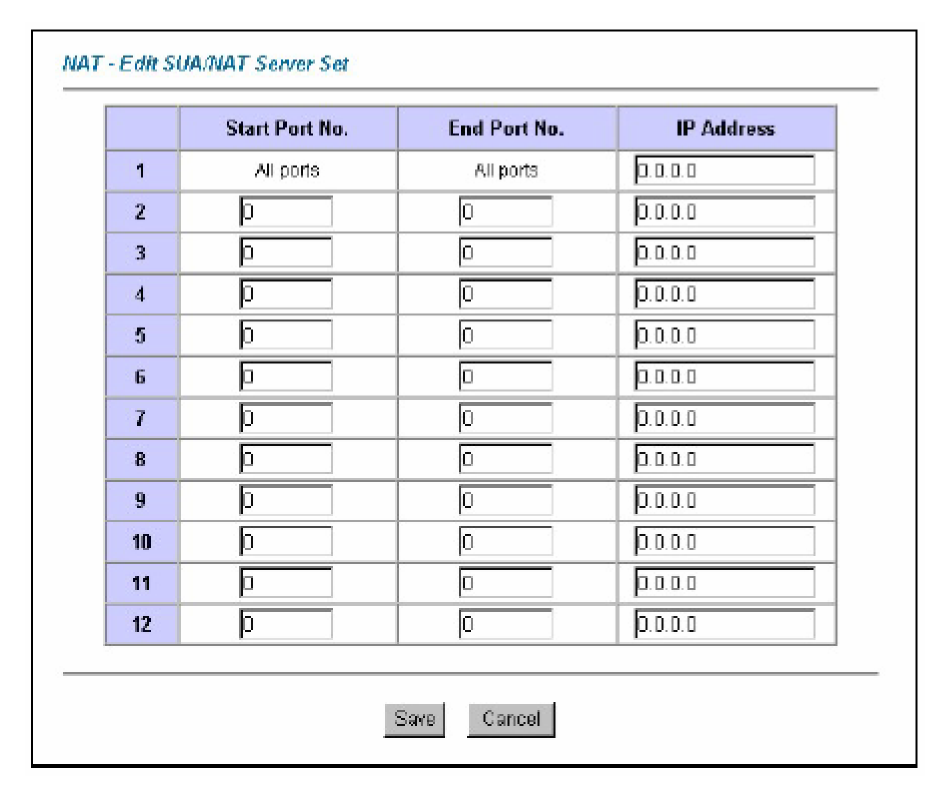


Figura 8-5 Editar el SUA/NAT Server Set

La siguiente tabla describe los campos de esta pantalla.

Tabla 8-5 Editar SUA/NAT Server Set

ETIQUETA	DESCRIPCIÓN
Stara Port No.	Introduzca el número de puerto en este campo. Para habilitar sólo un puerto, introduzca el número de puerto nuevamente en el campo **End Port No.** Para habilitar una serie de puertos, introduzca el número de puerto de inicio aquí y el número de puerto final en el campo **End Port No.**
End Port No.	Introduzca el número de puerto en este campo. Para habilitar sólo un puerto, introduzca el número de puerto nuevamente en el campo **Start Port No.** y a continuación introdúzcalo en este campo.

	Para habilitar una serie de puertos, introduzca el número de final del rango aquí y el número de puerto inicial en el campo **Stara Port No.**
Server IP Address	Introduzca la dirección IP del servidor en este campo
Save	Pulse **Save** para guardar los cambios en el Prestige
Cancel	Pulse **Cancel** para volver a los parámetros anteriores

8.6 Configurar Mapeos de Direcciones

El ordenar las reglas es importante porque el Prestige aplica las reglas en el orden en el que se especifican. Cuando un paquete cumple con una regla, el Prestige lleva a cabo la correspondiente acción y las reglas restantes son ignoradas. Si existe alguna regla vacía antes de la nueva regla configurada, la regla que se configure será colocada delante de estas reglas vacías. Por ejemplo, si tiene configuradas de las reglas 1 a la 6 y a continuación configura la regla número 9. En la pantalla resumen de las reglas, la nueva regla estará en el número 7, no en el 9. Si a continuación elimina la regla 4, las reglas 5 a 7 serán subidas un puesto, de manera que las antiguas reglas 5, 6 y 7 serán las nuevas 4, 5 y 6.

Para cambiar la configuración del Mapeo de Direcciones en su Prestige, pulse sobre **NAT**, seleccione **Full Feature** y haga clic sobre **Edit Details** para abrir la siguiente pantalla.

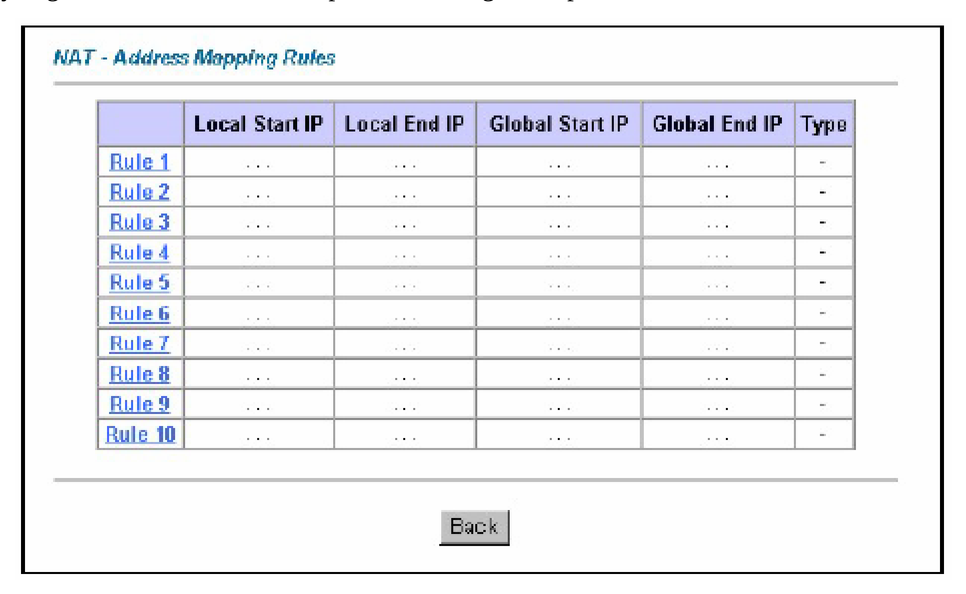


Figura 8-6 Reglas de Mapeo de Direcciones

La siguiente tabla describe los campos de esta pantalla.

Tabla 8-6 Reglas de Mapeo de Direcciones

ETIQUETA	DESCRIPCIÓN
Local Start IP	Ésta es la dirección interna local inicial. Las direcciones IP Locales son **N/A** para tipos de mapeo **Server**
Local End IP	Ésta es la dirección interna local final. Si la regla se define para todas las dirección IP locales, entonces se mostrará 0.0.0.0 en el campo **Local Start IP** y 255.255.255.255 como **Local End IP**. Este campo aparece como **N/A** para mapeos del tipo **One-to-One** y **Server**.
Global Start IP	Ésta es la dirección interna global de inicio. Introduzca 0.0.0.0 si la dirección IP se le asigna dinámicamente desde su ISP.
Global End IP	Ésta es la dirección interna global final. Este campo estará en **N/A** para los mapeos **One-to-One**, **Many-to-One** y **Server**.
Type	**1-1**: El modo One-to-One mapea una dirección IP local a una dirección IP global. Nótese que el número de puerto no se modificará para mapeos del tipo One-to-One. **M-1** : El modo Many-to-One mapea múltiples direcciones IP locales en una única dirección IP global. Esto es equivalente al SUA (p.e, PAT, port address translation), la única funcionalidad que los equipos de ZyXEL soportaban anteriormente. **M-M Ov** (Overload) : El modo Many-to-Many Overload mapea múltiples dirección IP locales en direcciones IP globales compartidas. **M-M No** (No Overload) : El modo Many-to-Many No Overload mapea cada dirección IP local en una única dirección IP global. **Server** : Este modo permite especificar servidores internos de manera que diversos servicios tras el NAT sean accesibles desde el exterior
Back	Pulse **Back** para volver a la pantalla **NAT Mode**

8.7 Editar una Regla del Address Mapping

Para editar una regla del mapeo de direcciones, pulse sobre el enlace de la regla en la pantalla NAT Address Mapping Rules para mostrar la siguiente pantalla.

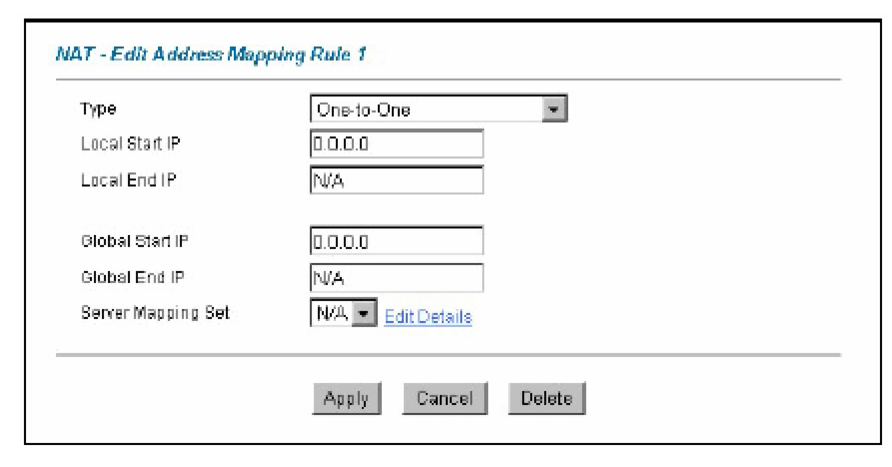


Figura 8-7 Editar una Regla del Mapeo de Direcciones

La siguiente tabla describe los campos de esta pantalla.

Tabla 8-7 Editar una Regla del Mapeo de Direcciones

ETIQUETA	DESCRIPCIÓN
Type	Seleccione el tipo del mapeo de direcciones de entre los siguientes: **1-1**: El modo One-to-One mapea una dirección IP local a una dirección IP global. Nótese que el número de puerto no se modificará para mapeos del tipo One-to-One. **M-1** : El modo Many-to-One mapea múltiples direcciones IP locales en una única dirección IP global. Esto es equivalente al SUA (p.e, PAT, port address translation), la única funcionalidad que los equipos de ZyXEL soportaban anteriormente. **M-M Ov** (Overload) : El modo Many-to-Many Overload mapea múltiples dirección IP locales en direcciones IP globales compartidas. **M-M No** (No Overload) : El modo Many-to-Many No Overload mapea cada dirección IP local en una única dirección IP global.

	Server : Este modo permite especificar servidores internos de manera que diversos servicios tras el NAT sean accesibles desde el exterior
Local Start IP	Ésta es la dirección IP local de inicio. Las direcciones IP locales estarán a **N/A** para el tipo de mapeo **Server**.
Local End IP	Ésta es la dirección IP local final. Si la regla hace referencia a todas las direcciones IP, entonces introduzca 0.0.0.0 como dirección en **Local Start IP** y 255.255.255.255 en la dirección **Local End IP** Este campo estará en **N/A** para mapeos del tipo **One-to-One**.
Global Start IP	Ésta es la dirección IP global de inicio. Introduzca 0.0.0.0 si su ISP asigna la dirección automáticamente.
Global End IP	Ésta es la dirección IP global final. Este campo estará a **N/A** para los mapeos **One-to-One, Many-to-One** y **Server**.
Server Mapping	Sólo disponible cuando el campo **Type** está en **Server**. Seleccione un número de la lista desplegable para seleccionar el conjunto de servidores de la pantalla **NAT – Address Mapping Rules**.
Edit Details	Pulse sobre este enlace para ir a la pantalla **NAT – Edit SUA/NAT Server Set** para editar el conjunto de servidores que se ha seleccionado en el campo **Server Mapping Set**.
Apply	Pulse sobre **Apply** para guardar los cambios en el Prestige.
Cancel	Pulse sobre **Cancel** para volver a los parámetros previamente guardados.
Delete	Pulse **Delete** para salir de esta pantalla sin guardar los cambios.

Capítulo 9
Configuración DNS Dinámico

Este capítulo describe como configurar su Prestige para utilizar el servicio DNS Dinámico

9.1 DNS Dinámico

La funcionalidad del DNS Dinámico le permite actualizar su dirección IP pública dinámica con uno o varios nombres de dominio de manera que cualquiera pueda acceder a su dispositivo (utilizando NetMeeting, etc.) Igualmente se podrá acceder a un servidor FTP o sitio Web instalados en su propio ordenador utilizando un nombre de dominio (por ejemplo myhost.dhs.org, donde myhost es un nombre a elegir) que nunca cambiará en lugar de una dirección IP dinámica que puede cambiar cada vez que se conecte. A sus amigos o conocidos siempre les será posible contactar con usted aunque no tengan conocimiento de cuál es la IP pública que tiene asignada.

En primer lugar, necesitará tener registrada una cuenta DNS dinámica en www.dyndns.org. Esto será útil para personas con una dirección IP dinámica suministrada por su ISP. El proveedor de servicio DNS Dinámico le proporcionará una clave o contraseña.

9.1.1 DYNDNS Wildcard

Habilitando la funcionalidad wildcard para su máquina hará que *.yourhost.dyndns.org sea asociado a la misma dirección IP que yourhost.dyndns.org. Esta funcionalidad es útil si se desea ser capaz de utilizar , por ejemplo, www.yourhost.dyndns.org y a la vez seguir pudiendo alcanzar la propia máquina.

Si dispone de una dirección IP privada en la WAN, no podrá utilizar la funcionalidad DNS Dinámica.

9.2 Configuración del DNS Dinámico

Para cambiar las propiedades DDNS del Prestige, pulse sobre DNS Dinámico (Dynamic DNS). La pantalla que aparece es:

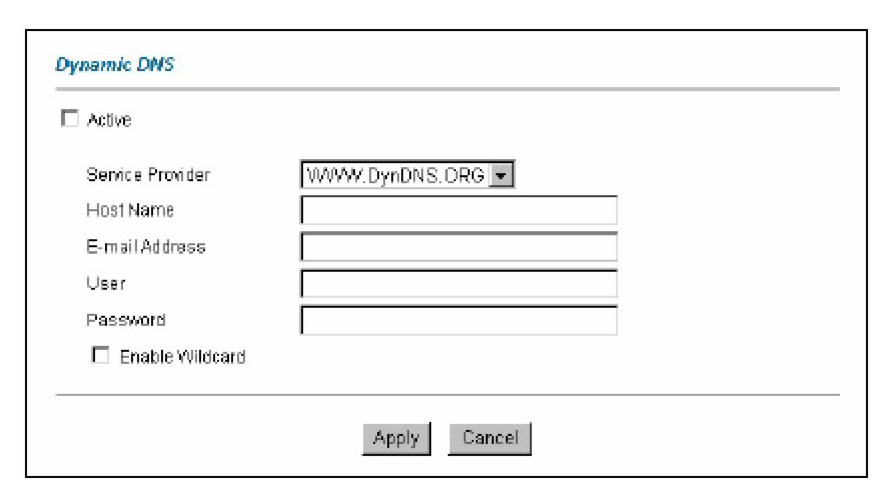


Figura 9-1 DDNS

La siguiente tabla describe los campos de esta pantalla.

Tabla 9-1 DDNS

ETIQUETA	DESCRIPCIÓN
Active	Seleccione esta casilla para utilizar el servicio DNS Dinámico
Service Provider	Éste es el nombre del proveedor de servico DNS Dinámico
Host Names	Introduzca el nombre de dominio asignado a su Prestige por el proveedor de DNS Dinámico
E-mail Address	Introduzca su dirección de correo
User	Introduzca su nombre de usuario
Password	Introduzca la contraseña que se le ha asignado
Enable Wildcard	Seleccione esta casilla para habilitar el servicio DYNDNS Wildcard
Apply	Pulse **Apply** para guardar los cambios al Prestige
Cancel	Pulse **Cancel** para comenzar a configurar esta pantalla de nuevo

Capítulo 10
Fecha y Hora

Esta pantalla no está disponible en todos los modelos. Utilice la misma para configurar los parámetros de fecha y hora del Prestige.

10.1 Configuración Fecha y Hora

Para modificar los parámetros de fecha y hora del Prestige, pulse sobre Fecha y Hora (Time And Date). Aparecerá la siguiente pantalla. Utilícela para configurar la hora del Prestige basada en su zona horaria local.

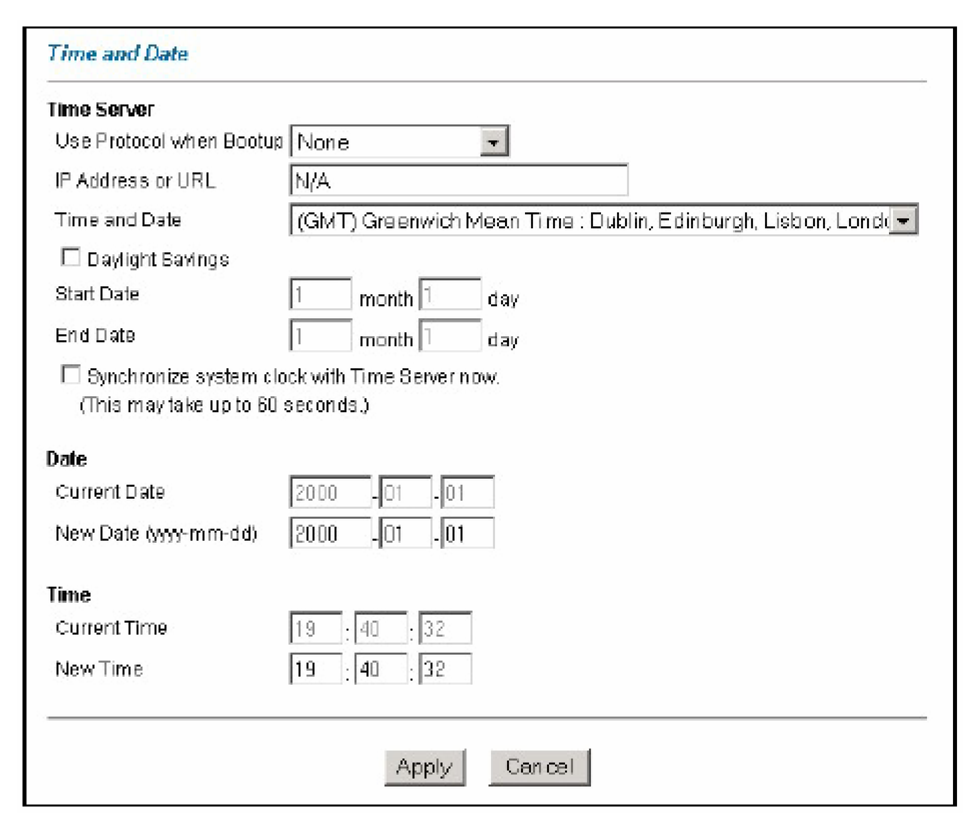


Figura 10-1 Fecha y Hora

La siguiente tabla describe los campos de esta pantalla.

Tabla 10-1 Fecha y Hora

ETIQUETA	DESCRIPCIÓN
Time Server	
Use Protocol when Bootup	Seleccione un protocolo de servicio de tiempo que su servidor de tiempo envía cuando se enciende el Prestige. No todos los servidores de tiempo soportan todos los protocolos, de manera que será necesario verificarlo con el ISP/administrador de red o utilizar un mecanismo de prueba y error para encontrar un protocolo que funcione. La principal diferencia entre ellos es el formato. El formato **Daytime (RFC 867)** es día/mes/año/zona horaria del servidor El formato **Time (RFC 868)** muestra un entero de 4 bytes con el número total de segundos desde las 0:0:0 del 1/1/1970 Por defecto, **NTP(RFC 1305)**, similar al **Time (RFC 868).** Seleccione **None** para configurar la fecha y hora manualmente.
IP Address or URL	Introduzca la dirección IP o URL del servidor de tiempo. Compruebe con su ISP/Administrador de red si no está completamente seguro de este valor (por defecto es tick.stdtime.gov.tw)
Time and Date	Seleccione la zona horaria de su ubicación. Ésta será la diferencia entre su zona horaria y el tiempo del meridiano de Greenwich (GMT).
Daylight Savings	Seleccione esta opción si desea configurar horario de verano. El horario de verano es el periodo desde finales de primavera hasta principios de otoño donde muchos países adelantan sus relojes un hora respecto a la hora local habitual para disponer de más horas de luz solar por las tardes.
Start Date	Introduzca el mes y el día en que comienza el horario de verano si selecciona la opción **Daylight Savings**.
End Date	Introduzca el mes y el día en que finaliza el horario de verano si selecciona la opción **Daylight Savings**.
Synchronizce system clock with Time Server now.	Seleccione esta opción para que su Prestige utilice el servidor de tiempo (configurado más arriba) para configurar su reloj interno. Por favor, espere unos 60 segundos hasta que el Prestige localice el servidor de tiempo. Si el Prestige no puede localizarlo, por favor, compruebe el protocolo del servidor de tiempo y su dirección IP. Si la dirección IP se introdujo correctamente, prueba a hacer ping al mismo para testear la conexión.

Date	
Current Date	Este campo muestra la fecha de su Prestige. Cada vez que se refresque esta pantalla, el Prestige sincroniza el tiempo con el servidor de tiempo.
New Date (yyyy-mm-dd)	Este campo muestra la última fecha actualizada desde el servidor de tiempo. Cuando se selecciona **None** en el campo **Use Protocol when Bootup**, introduzca la fecha actual en este campo y después pulse **Apply**.
Time	
Current Time	Este campo muestra el tiempo de su Prestige. Cada vez que se refresque esta pantalla, el Prestige sincroniza la hora con el servidor de tiempo.
New Time	Este campo muestra la última hora actualizada desde el servidor de tiempo. Cuando selecciona **None** en el campo **Use Protocol when Bootup**, introduzca la nueva hora en este campo y pulse sobre **Apply.**
Apply	Pulse **Apply** para guardar los cambios en su Prestige.
Cancel	Pulse **Cancel** para comenzar a configurar esta pantalla de nuevo.

Capítulo 11
Configuración Gestión Remota

Este capítulo proporciona información sobre como configurar la gestión remota.

11.1 Descripción Gestión Remota

La gestión remota permite el determinar que servicios/protocolos pueden acceder a través de los interfaces al Prestige y desde que ordenadores.

Se podrá gestionar el Prestige desde una ubicación remota a través de:

- Internet (Sólo WAN)
- ALL (Tanto LAN como WAN)
- Sólo LAN
- Neither (Deshabilitada)

Para deshabilitar la gestión remota a través de un servicio, seleccione **Deshabilitar (Disable)** en el campo correspondiente del campo **Servicio de Acceso (Server Access).**

Únicamente será posible una sesión de gestión simultánea. El Prestige automáticamente desconecta una sesión de gestión de inferior prioridad cuando se ejecuta otra sesión de gestión con prioridad más elevada. Las prioridades de los diferentes tipos de gestión se indican a continuación:

1.- Telnet

2.- HTTP

11.1.1 Limitaciones de la Gestión Remota

La gestión sobre LAN o WAN no funcionará cuando:

1. Se encuentre aplicado bien en el menú 3.1 (LAN) o en el menú 11.5 (WAN) un filtro para bloquear el tráfico Telnet, FTP o Web.
2. Se haya deshabilitado el servicio en una de las pantallas de gestión remota.
3. La dirección IP en el campo Cliente IP Seguro (Secured Client IP) no coincida con la dirección IP del cliente. Si no existe coincidencia, el Prestige desconectará la sesión inmediatamente.

4. Existe ya otra sesión de gestión con igual o mayor prioridad. Únicamente es posible tener una sesión de gestión ejecutándose simultáneamente.

11.1.2 Gestión remota y NAT

Cuando el NAT está habilitado:

- Utilice la dirección IP de la WAN del Prestige cuando se esté configurando desde el lado WAN.
- Utilice la dirección IP de la LAN del Prestige cuando se esté configurando desde el lado LAN.

11.1.3 Temporización de inactividad del sistema

Existe un temporizador de inactividad de gestión del sistema, por defecto, a 5 minutos (300 segundos). El Prestige automáticamente desconecta automáticamente la sesión que permanece inactiva más de este periodo. La sesión de gestión no expira nunca cuando está mostrando una pantalla de estadísticas.

11.2 Telnet

Es posible configurar el Prestige para acceso remoto via Telnet como se muestra a continuación.

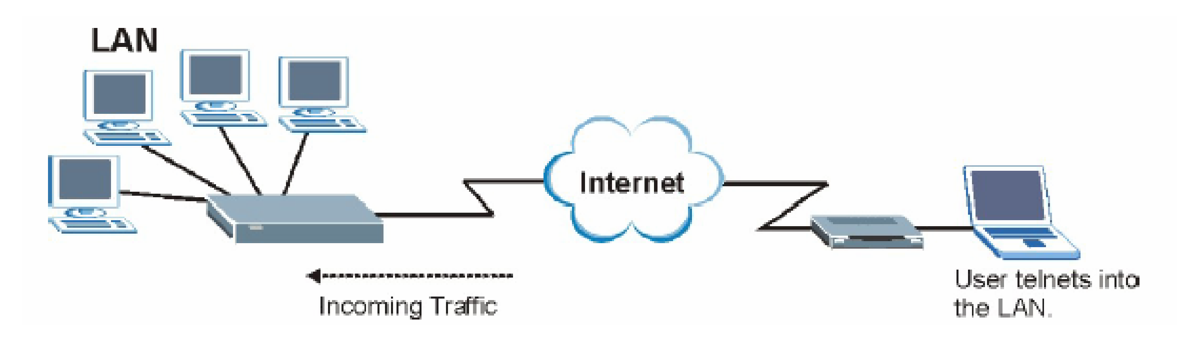


Figura 11-1 Configuración Telnet en una red TCP/IP

11.3 FTP

Será posible actualizar el firmware del Prestige o actualizar o hacer un backup de la configuración utilizando la transferencia FTP. Para utilizar esta funcionalidad, sus ordenadores deberán contemplar un cliente FTP.

11.4 WEB

Es posible utilizar el configurador web integrado en el Prestige para la gestión y configuración. Consulte la ayuda online para más detalles.

11.5 Configuración de la Gestión Remota

Pulse sobre Remote Management para abrir la siguiente pantalla.

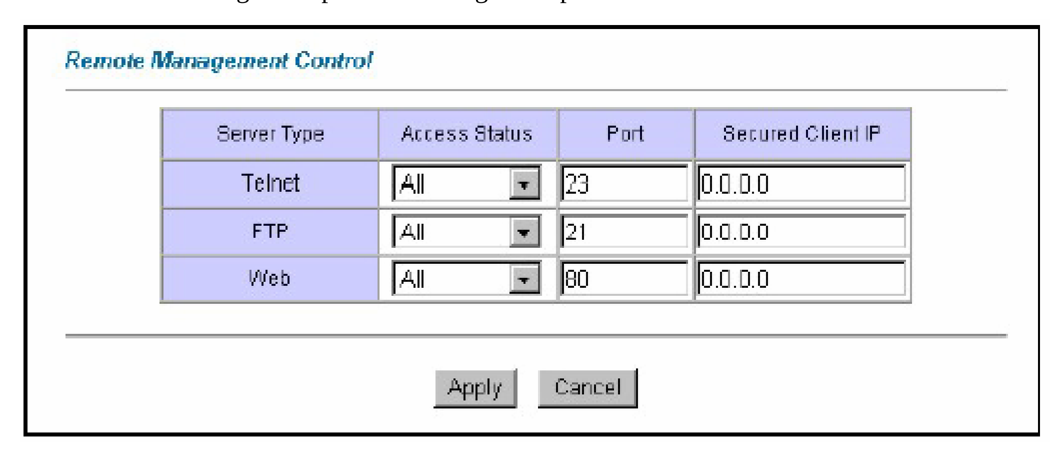


Figura 11-2 Gestión Remota

La siguiente tabla describe los campos de esta pantalla.

Tabla 11-1 Gestión Remota

ETIQUETA	DESCRIPCIÓN
Server Type	Cada uno de estas etiquetas denota el servicio que se podrá utilizar para la gestión remota del Prestige.
Access Status	Seleccione el interfaz de acceso. Escoga entre **All (Todos), LAN Only (Sólo LAN), WAN Only (Sólo WAN)** y **Disable (Deshabilitado)**.
Port	Este campo muestra el número de puerto para el servicio de gestión remota. Será posible modificar el número del puerto para este servicio en este campo.
Secured Client IP	Por defecto 0.0.0.0 permite que cualquier cliente utilice este servicio para gestionar el Prestige. Introduzca una dirección IP para restringir el acceso a un cliente cuya IP coincida con la configurada.
Apply	Pulse **Apply** para guardar los cambios.

Cancel	Pulse **Cancel** para volver a configurar la pantalla de nuevo.

Asimismo, cuando se desee que determinado tipo de tráfico proveniente desde internet sea aceptado por el router (tanto para propósitos de gestión como en situaciones en la que se disponga de algún servidor interno), se deberá verificar que los parámetros configurados en la pantalla Internet Security se encuentran correctamente configurados para posibilitar el acceso al tráfico del protocolo deseado procedente de internet.

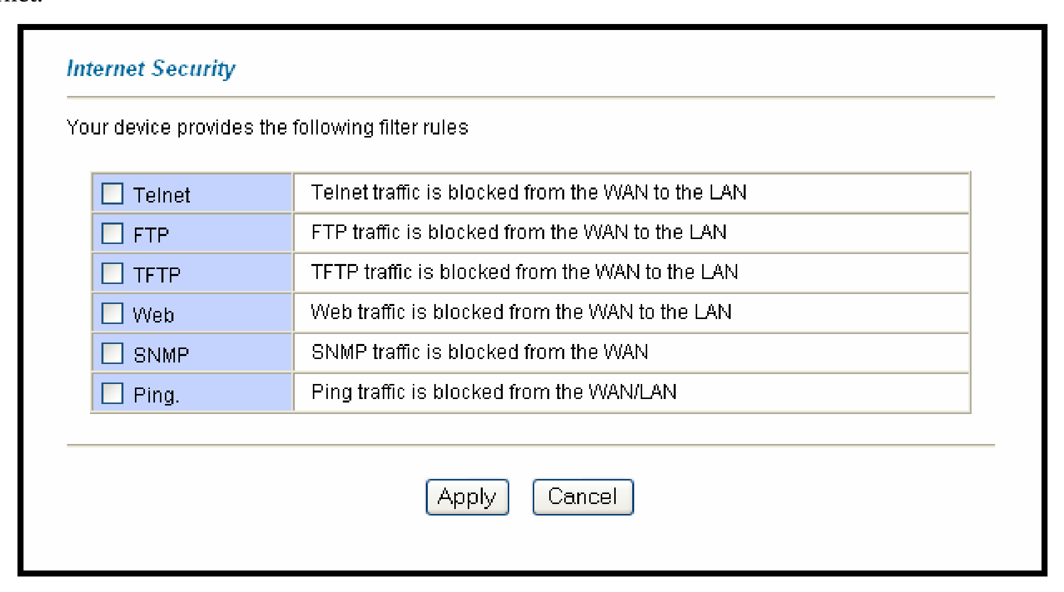


Figura 11.3 – Reglas de seguridad

Capítulo 12
Universal Plug-and-Play (UPnP)

Este capítulo introduce la funcionalidad UpnP del configurador web.

12.1 Introducción al Universal Plug and Play

Universal Plug and Play (UPnP) es un estándar distribuido, abierto que utiliza TCP/IP para la conectividad entre dispositivos. Un dispositivo UPnP puede unirse dinámicamente a una red, obtener una dirección IP, compartir sus capacidades y aprender acerca de otros dispositivos de la red. Adicionalmente, un dispositivo puede dejar una red automáticamente cuando no se encuentre en uso.

12.1.1 ¿Cómo saber si se está utilizando UPnP?

El hardware UPnP se identifica con un icono en la carpeta de Conexiones de Red (Windows XP). Cada dispositivo UPnP compatible instalado en la red aparecerá con un icono separado. Seleccionando el icono de un dispositivo UPnP podrá acceder a la información y propiedades del mismo.

12.1.2 NAT Traversal

UPnP NAT Traversal automatiza el proceso de permitir a una aplicación operar a través del NAT. Los dispositivos de red UPnP pueden configurar automáticamente el direccionamiento de red, anunciar su presencia en la red a otros dispositivos UPnP y habilitar el intercambio de descripciones de servicio sencillas. El NAT Traversal ofrece lo siguiente:

- Mapeo de puertos dinámico
- Aprendizaje de direcciones IP públicas
- Asignación de temporizadores a los mapeos.

Windows Messenger es un ejemplo de aplicación que soporta NAT Traversal y UPnP.

Consulte el capítulo de NAT para más información sobre dicha funcionalidad.

12.1.3 Precauciones con el UPnP

La naturaleza automática de las aplicaciones NAT Traversal para establecer sus propios servicios puede presentar problemas de seguridad en las redes. La información de red y la configuración podría ser obtenida y modificada por usuarios en algunos entornos de red.

Todos los dispositivos con UPnP habilitado podrán comunicarse libremente entre ellos sin ninguna configuración adicional. Deshabilite el UPnP si ésta no es su intención.

12.2 UPnP y ZyXEL

ZyXEL ha logrado la certificación UPnP del Universal Plug and Play Forum Creates UPnP^{TM} Implementers Corp. (UIC). La implementación UPnP de ZyXEL soporta IGD 1.0 (Internet Gateway Device). En el momento de escribir este documento la implementación UPnP de ZyXEL soporta Windows Messenger 4.6 y 4.7 mientras que el Windows Messenger 5.0 y XBOX están todavía en pruebas.

El broadcast UPnP sólo está permitido en la LAN.

Consulte secciones posteriores para ver ejemplos sobre la instalación del UPnP en Windows XP y Windows Me así como un ejemplo del uso del UPnP en Windows.

12.2.1 Configuración UPnP

Desde el menú principal **Site Map**, pulse sobre **UPnP** bajo el menú **Advanced Setup** para mostrar la siguiente pantalla.

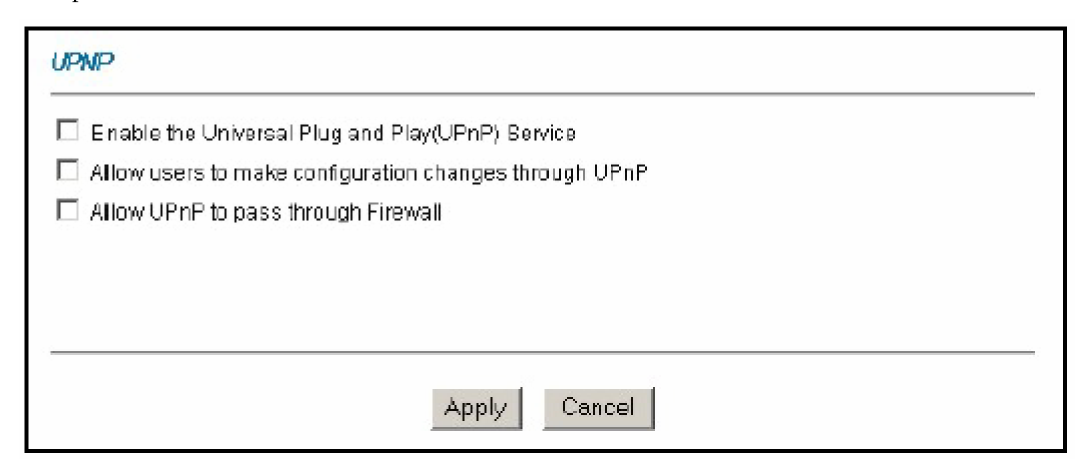


Figura 12-1 Configuración UPnP

La siguiente tabla describe los campos de esta pantalla.

Tabla 12-1 Configuración UPnP

ETIQUETA	DESCRIPCIÓN
Enable the Universal Plug and Play (UPnP) Service	Seleccione esta casilla para activar el UPnP. Tenga la precaución de que cualquiera podrá utilizar la aplicación UPnP para abrir la pantalla de acceso del configurador web sin introducir la dirección IP del Prestige (aunque todavía será necesario introducir la contraseña para acceder al configurador web).
Allow users to make configuration changes through UPnP	Seleccione esta casilla para permitir que la aplicaciones UPnP configuren automáticamente de manera que puedan comunicarse a través del Prestige, por ejemplo utilizando NAT Traversal, las aplicaciones UPnP automáticamente reservan unos puertos de envío en la tabla NAT para comunicarse con otros dispositivos con el UPnP habilitado; esto elimina la necesidad de configurar manualmente el mapeo de puertos para las aplicaciones con el UPnP habilitado.
Apply	Pulse **Apply** para guardar los cambios.
Cancel	Pulse **Cancel** para volver a los parámetros previamente almancenados.

12.3 Ejemplo de Instalación UPnP en Windows

Esta sección muestra como instalar UPnP en Windows Me y Windows XP.

Instalación UPnP en Windows Me

Paso 1. Pulse **Inicio** y **Panel de Control**. Doble-click en **Agregar/Quitar programas**.

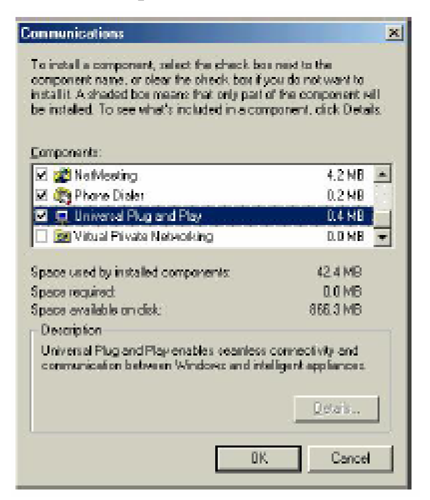
Paso 2. Pulse en la pestaña de **Configuración de Windows** y seleccione **Comunicaciones** en la casilla de selección de **Componentes**. Pulse **Detalles**.



Paso 3. En la pantalla **Comunicaciones**, seleccione la casilla **Universal Plug and Play** en la caja de **Componentes**.

Paso 4. Pulse sobre Aceptar para volver a la pantalla de Propiedades de Agregar/Quitar Programas y pulse sobre Siguiente.

Paso 5. Reinicie el ordenador cuando se le pida.



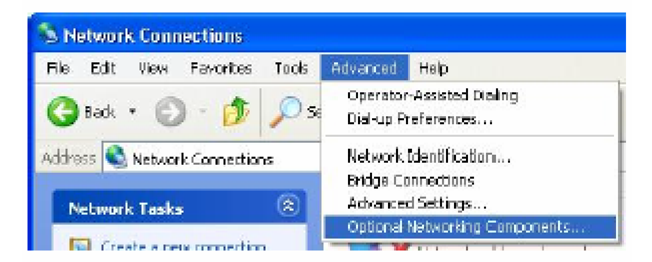
Instalación UPnP en Windows XP

Siga los siguientes pasos para instalar UPnP en Windows XP.

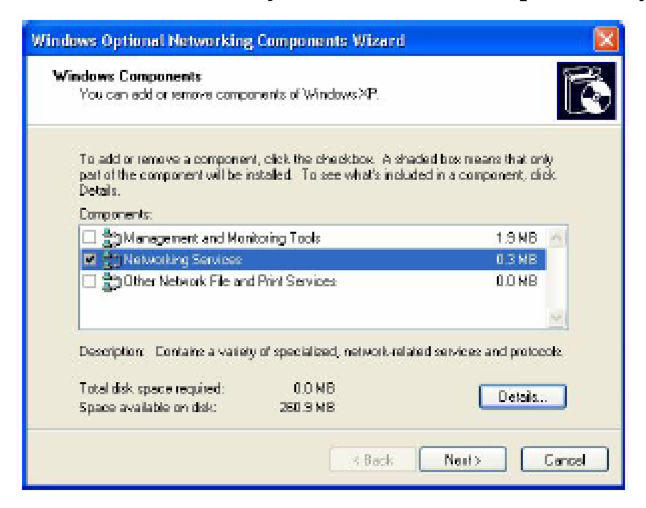
Paso 1. Pulse **Inicio** y **Panel de Control**.

Paso 2. Doble-click en **Conexiones de Red**

Paso 3. En la ventana de **Conexiones de Red**, pulse sobre **Opciones Avanzadas** en el menú principal y seleccione **Componentes de Red Opcionales…** Se mostrará la ventana del **Asistente de Componentes Opcionales de Red**.

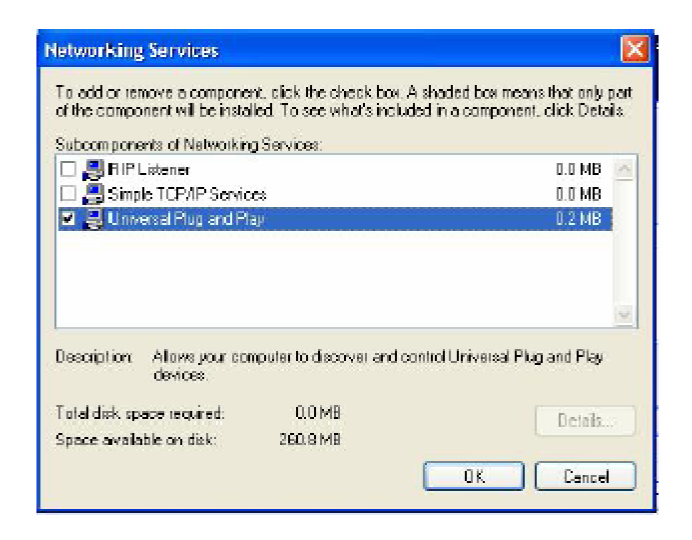


Paso 4. Seleccione **Servicios de Red** en la caja de selección de **Componenetes** y pulse sobre **Detalles**.



Paso 5. En la ventana de **Servicios de Red**, seleccione la casilla de **Universal Plug and Play**.

Paso 6. Pulse **Aceptar** para volver a la ventana del **Asistente de Componentes Opcionales de Red** y pulse **Siguiente**.



12.4 Ejemplo Utilización UPnP en Windows XP

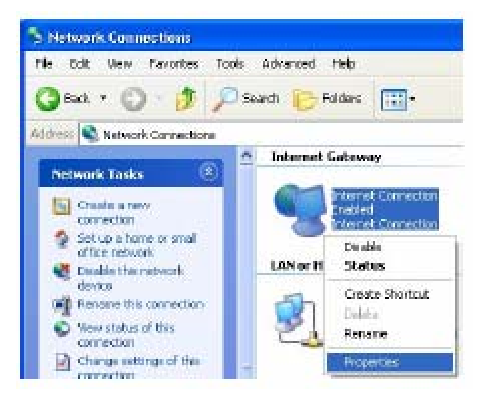
Esta sección muestra como utilizar la funcionalidad UPnP en Windows XP. Debe disponer del UPnP instalado en Windows XP y activado en el Prestige.

Igualmente asegúrese que el ordenador está conectado al puerto LAN del Prestige. Encienda su ordenador y el Prestige.

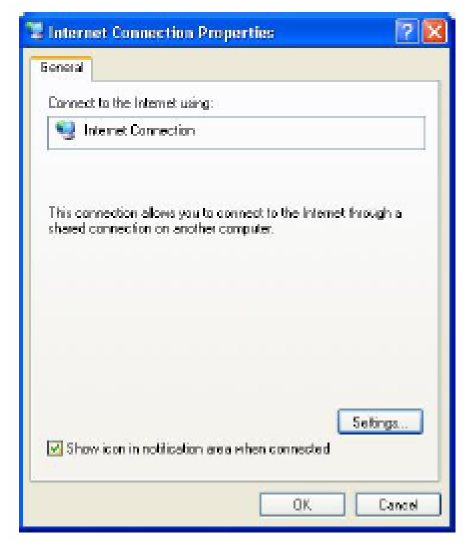
Auto-descubrir los dispositivos de red UPnP

Paso 1. Pulse sobre **Inicio** y **Panel de Control**. Doble-click en **Conexiones de Red**. Un icono aparecerá en el apartado de Puerta de enlace de Internet.

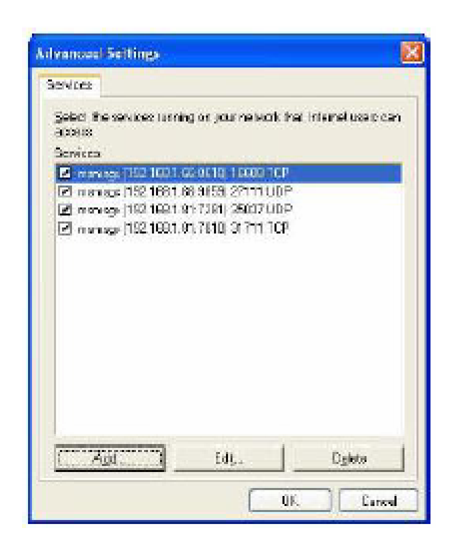
Paso 2. Pulse con el botón derecho del ratón en el icono y seleccione **Propiedades**.

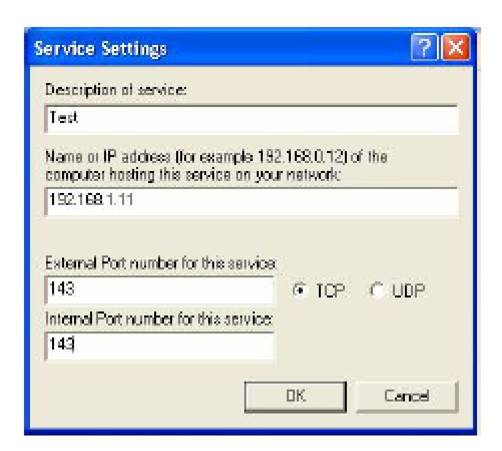


Paso 3. En la ventana de **Propiedades de Conexión a Internet**, pulse sobre **Configuración** para ver los mapeos de puertos que han sido creados automáticamente.



Paso 4. Deberá editar o borrar el mapeo de puertos o pulsar sobre **Agregar** para añadir mapeos de puertos manualmente.



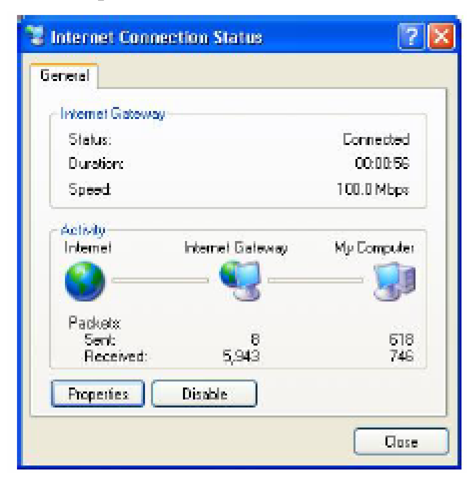


Cuando los dispositivos UPnP se desconectan de la red, todos los mapeos de puertos serán eliminados automáticamente.

Paso 5. Seleccione la opción **Mostrar icono en el área de notificación al conectarse** y pulse **Aceptar**. Un icono aparecerá en la barra de tareas del sistema.



Paso 6. Haga doble-click en el icono para mostrar el estado de la conexión a Internet actual.



Configurador Web de Fácil Acceso

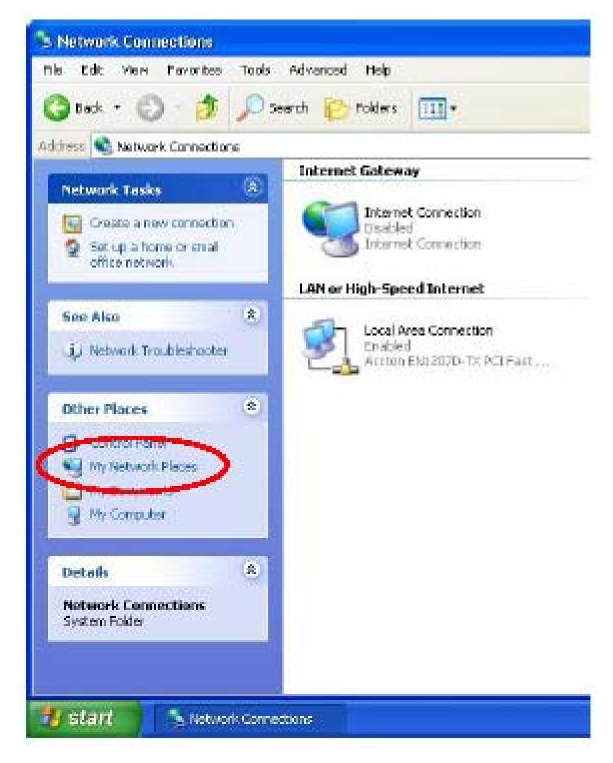
Con UPnP, es posible acceder al configurador basado en web del Prestige sin necesidad de conocer la dirección IP del Prestige. Esto es útil en caso de desconocimiento de la dirección IP del Prestige.

Siga los siguientes pasos para acceder al configurador web.

Paso 1. Pulse sobre **Inicio** y **Panel de Control**.

Paso 2. Doble-click en **Conexiones de Red**.

Paso 3. Seleccione **Mis Sitios de Red** bajo **Otros sitios**.

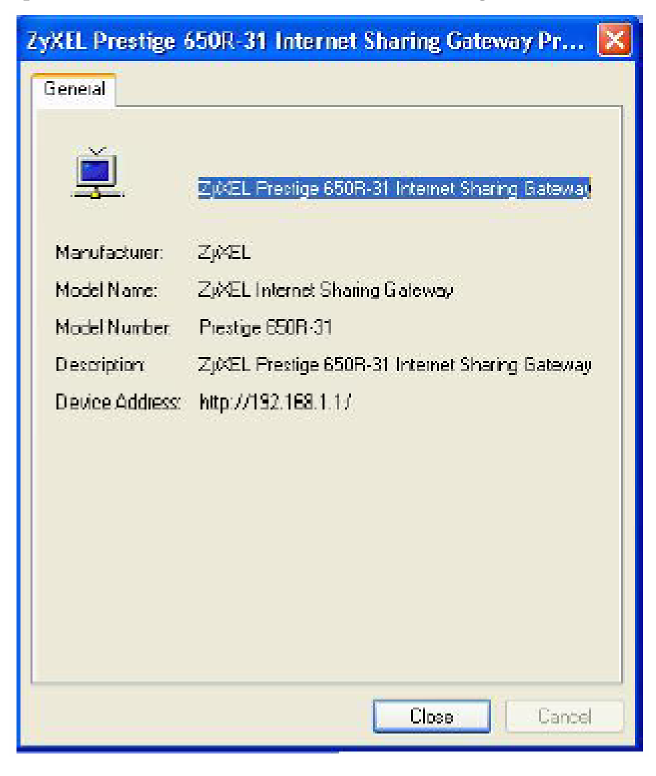


Paso 4. Un icono con la descripción de cada dispositivo UPnP se muestra bajo **Red Local.**

Paso 5. Pulse con el botón derecho del ratón en el icono del Prestige y seleccione **Abrir**. La pantalla de acceso al configurador web aparecerá.



Paso 6. Pulse con el botón derecho del ratón de su Prestige y seleccione **Propiedades**. Una ventana de propiedades aparecerá con información básica del Prestige.



Capítulo 13
Pantallas de Registros

Este capítulo contiene información sobre la configuración general de los parámetros del registro y la visualización de los logs del Prestige. Consulte el apéndice para explicaciones sobre los mensajes de los logs.

13.1 Descripción de Logs

El configurador web permite elegir que categorías de eventos y/o alertas el Prestige podrá registrar y mostrarlos o hacer que el Prestige los envíe a un administrador (via e-mail) o a un servidor syslog.

13.1.1 Alertas y Logs

Una alerta es un tipo de registro que necesita una atención más seria. Incluyen errores del sistema, ataques (control de acceso) e intentos de acceso a sitios web bloqueados. Algunas categorías tales como **Errores del Sistema (System Errors)** consisten tanto en registros como alertas. Podrán ser diferenciados mediante el color en la ventana del **Visualización del Log (View Log)**. Las alertas se muestran en rojo y los logs en negro.

13.2 Configuración de los parámetros del Log

Utilice la pantalla **Configuración del Log (Log Settings)** para configurar en el Prestige donde enviar los logs; el horario cuando debe enviarlos y que logs y/o alertas deben ser almacenadas.

Para modificar los parámetros de configuración del Prestige, pulse sobre **Logs**, y **Log Settings**. La pantalla aparece como se muestra.

Las alertas son enviadas via e-mail tan pronto como se producen. Los logs se pueden enviar tan pronto como la tabla de registro esté llena (consultar **Log Schedule – Horario de Logs**). El seleccionar muchas categorías de alertas y/o logs (especialmente de **Control de Acceso – Access Control**) puede originar el envío de muchos mails.

Logs - Log Settings

Address Info:

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject:

Send log to: (E-Mail Address)

Send alerts to: (E-Mail Address)

UNIX Syslog:

☐ Active

Syslog IP Address: 0.0.0.0 (Server Name or IP Address)

Log Facility: Local 1

Send Log:

Log Schedule: When Log is Full

Day for Sending Log: Monday

Time for Sending Log: 0 (hour): 0 (minute)

Log	Send immediate alert
☐ System Maintenance	☐ System Errors
☐ System Errors	☐ Blocked Web Sites
☐ Access Control	☐ Attacks
☐ UPnP	
☐ Forward Web Sites	
☐ Blocked Web Sites	
☐ Attacks	
☐ IPSec	
☐ IKE	

Back Apply Cancel

Figura 13-1 Configuración de Logs

La siguiente tabla describe los campos de esta pantalla.

Tabla 13-1 Configuración de Logs

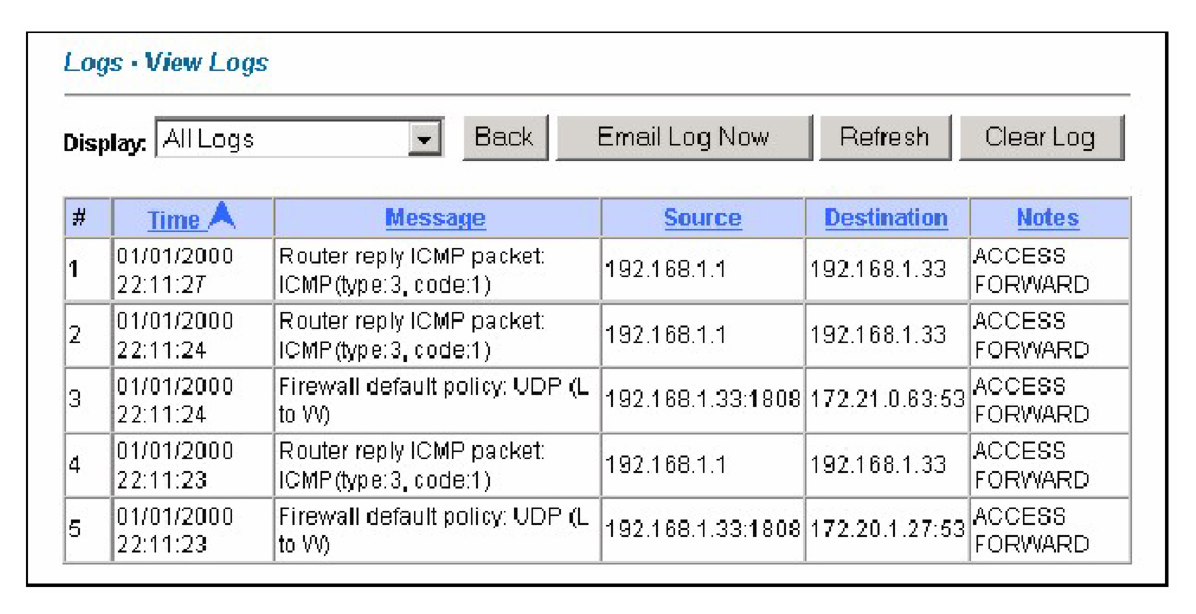
ETIQUETA	DESCRIPCIÓN
Address Info	
Mail Server	Introduzca el nombre del servidor o la dirección IP del servidor de correo para las direcciones de correo especificadas a continuación. Si el campo se deja en blanco, los mensajes de logs y alertas no se enviará por correo.
Mail Subject	Introduzca un título que desea que aparezca como el asunto del mensaje que el Prestige envíe.
Send log to	Los logs se envían a la dirección de correo especificada en este campo. Si se deja el campo en blanco, los logs no se enviarán a través del mail.
Send alerts to	Las alertas se enviarán a la dirección especificada en este campo. Si el campo se deja en blanco, las alertas no serán enviadas via mail.
UNIX Syslog	Envío de logs a un servidor syslog externo utilizado para almacenarlos.
Active	Pulse Active para habilitar el registro de syslog.
Syslog IP Address	Introduzca el nombre del servidor o la dirección IP del servidor syslog que registrará las categorías de logs seleccionadas.
Log Facility	Seleccione una localización de la lista desplegable. La facilidad de log permite almacenar los mensajes en diferentes ficheros en el servidor syslog. Consulte la documentación de su programa syslog para más detalles.
Send Log	
Log Schedule	Este menú desplegable es usado para configurar la frecuencia a la que se envían los mensajes de logs como E-mail: • **Daily (Diariamente)** • **Weekly (Semanalmente)** • **Hourly (Cada hora)** • **When Log is Full (Cuando el registro esté lleno)** • **None (Nunca)** Si selecciona **Weekly** o **Daily**, especifique la hora del día en la que el correo debe ser remitido.

	Si selecciona **Weekly**, también deberá especificar el día de la semana en que el correo debe ser enviado. Si selecciona **When Log is Full**, se enviará el mensaje cuando el registro esté completo. Si selecciona **None**, no se enviará ningún mensaje de log.
Day for Sending Log	Utilice la lista desplegable para seleccionar el día de la semana en el que se enviarán los logs.
Time for Sending Log	Introduzca la hora del día en formato de 24 horas (por ejemplo 23:00 es igual a 11:00 pm) en la que enviar los logs.
Log	Seleccione las categorías de logs que desea registrar. Los logs incluyen las alertas.
Send Immediate Alert	Seleccione las categorías de alertas para las que desea que el Prestige debe enviar un mail instantáneamente a la dirección especificada en el campo **Send Alerts To**.
Back	Pulse Back para volver a la pantalla previa.
Apply	Pulse Apply para guardar los cambios en el equipo.
Cancel	Pulse Cancel para volver a los parámetros almacenados previamente.

13.3 Visualización de los Logs

Pulse **Logs** y a continuación **View Log** para abrir la pantalla de **Visualización de Logs (View Logs**). Utilice esta pantalla para ver los logs de las categorías seleccionadas en la pantalla de Configuración **de Logs (Logs Settings)** (ver sección 18.2).

Las entradas del logs en rojo indican alertas. Cuando la tabla de registro se completa vuelve a comenzar por el principio borrando las entradas más antiguas. Pulse sobre la cabecera de una columna para ordenar las entradas. Un triángulo indica el sentido ascendente o descendente del orden.



#	Time	Message	Source	Destination	Notes
1	01/01/2000 22:11:27	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
2	01/01/2000 22:11:24	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
3	01/01/2000 22:11:24	Firewall default policy: UDP (L to W)	192.168.1.33:1808	172.21.0.63:53	ACCESS FORWARD
4	01/01/2000 22:11:23	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
5	01/01/2000 22:11:23	Firewall default policy: UDP (L to W)	192.168.1.33:1808	172.20.1.27:53	ACCESS FORWARD

Figura 13-2 Visualización de Logs

La siguiente tabla describe los campos de esta pantalla.

Tabla 13-2 Visualización de Logs

ETIQUETA	DESCRIPCIÓN
Display	Las categorías seleccionadas en la **Configuración de Logs (Log Settings)** (ver sección 18.2) aparecen en la lista desplegable. Seleccione una categoría de logs para visualizarlos; seleccione **Todos los Logs (All Logs)** para ver los logs de todas las categorías ques se seleccionaron en la pantalla de **Configuración (Log Settings).**
Time	Este campo muestra el tiempo en que el log fue registrado. Consulte el capítulo de mantenimiento del sistema para más información sobre como configurar la fecha y hora del Prestige.
Message	Este campo indica la razón del log.
Source	Este campo lista la dirección IP origen y el número de puerto del paquete entrante.

Destination	Este campo indica la dirección IP destino y el número de puerto del paquete entrante.
Notes	Este campo muestra información adicional sobre la entrada del log.
Back	Pulse **Back** para volver a la pantalla previa.
Email Log Now	Pulse sobre **Email Log Now** para enviar el log a la dirección de email especificada en la página de **Configuración (Log Settings)** (asegúrese de que ha introducido una dirección en el campo **Address Info**, ver sección 18.2).
Refresh	Pulse **Refresh** para refrescar la página de logs.
Clear Log	Pulse **Clear Log** para borrar todos los logs.

Capítulo 14
Gestión de ancho de banda

Este capítulo describe la configuración avanzada de la gestión del ancho de banda

14.1 Descripción Gestión del Ancho de Banda

La gestión del ancho de banda permite reservar cierta capacidad del ancho de banda de salida de un determinado interfaz para determinados tipos de tráfico. Esto puede ayudar igualmente a asegurar que el router va a enviar siempre cierto tipo de tráfico (en especial aplicaciones de tiempo real) con un mínimo retardo. Dado el incremento en el uso de aplicaciones de tiempo real tales como la voz sobre IP (VoIP), los requerimientos de ancho de banda van también creciendo.

La gestión del ancho de banda tiene como objetivo responder a las siguientes cuestiones:

- ¿Quién debería obtener un determinado nivel de servicio para ciertas aplicaciones?
- ¿Qué nivel de prioridad debería asignarse a cada tipo de tráfico?
- ¿Para qué tipo de tráfico debe garantizarse su entrega?
- ¿Qué cantidad de ancho de banda debe ser reservada para garantizar un correcto funcionamiento?

La gestión del ancho de banda también permite la configuración del ancho de banda de salida permitido en un interfaz para su coincidencia con el que puede manejar la red. Esto ayuda a reducir los retardos y las pérdidas de paquetes en el siguiente dispositivo de enrutamiento. Por ejemplo, es posible configurar el interfaz WAN con una velocidad de 1000kbps si la conexión de ADSL dispone de una velocidad de subida de 1000kbps. Todas las pantallas de configuración muestran la medida en kbps, aunque en la guía de usuario también se utiliza la medida en Mbps.

14.2 Clases del Ancho de Banda y Filtros

Utilice la definición de clases en la gestión del ancho de banda para reservar cierto ancho de banda. La configuración de un filtro permite definir una clase en base a una aplicación específica y/o subred. Utilice la pantalla Class Configuration (consultar sección 14.9) para configurar el nombre de una clase, la reserva de ancho de banda y el filtro correspondiente. La información sobre las clases y los filtros configurados es accesible a través de la pantalla Class Setup (consultar sección 14.9).

El total del ancho de banda reservado para las clases no puede exceder del ancho de banda configurado para la clase raiz.

14.3 Reserva del Ancho de Banda

La gestión del ancho de banda permite definir que cantidad del ancho de banda puede obtener cada clase; sin embargo, el ancho de banda real para cada clase crece o decrece en proporción al ancho de banda real disponible.

14.4 Ejemplos Gestión de Ancho de Banda

Estos ejemplos muestran la reserva de ancho de banda en un interfaz WAN configurado con 640kbps.

14.4.1 Ejemplo Gestión de Ancho de Banda basado en aplicación

Las clases del siguiente ejemplo están definidas exclusivamente en base a aplicaciones. Cada clase (VoIP, Web,. FTP, E-mail y video) tienen reservado un ancho de 128kbps.

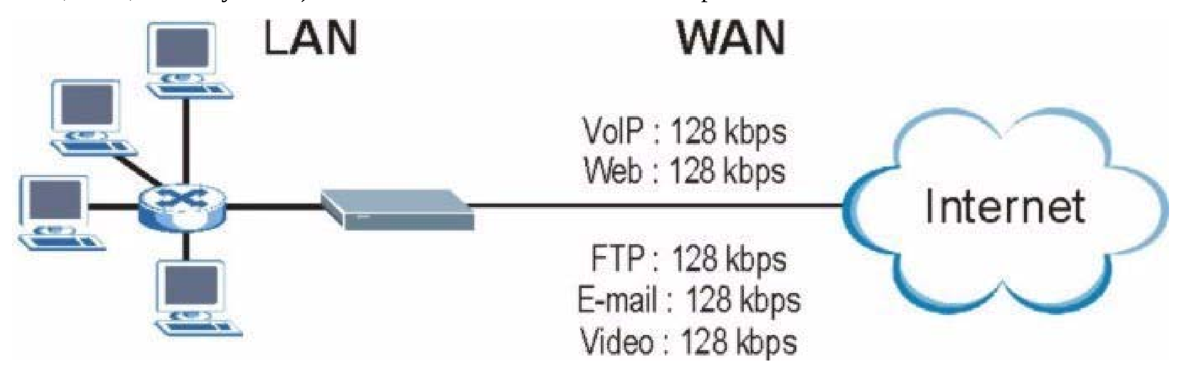


Figura 14-1 Ejemplo Gestión Ancho de Banda basado en Aplicaciones

14.4.2 Ejemplo de Gestión de Ancho de Banda basado en Subred

El siguiente ejemplo define las clases en base a subredes de LAN. Cada clase (Subnet A y Subnet B) tiene reservada un ancho de 320kbps.

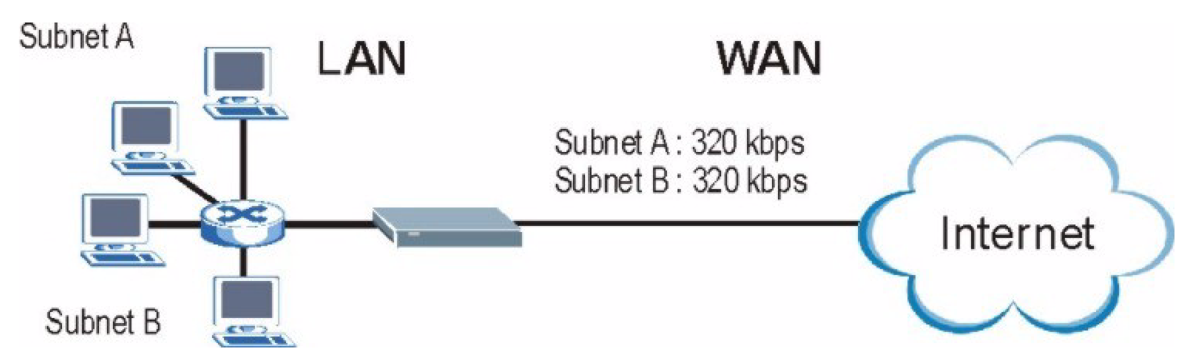


Figura 14-2 Ejemplo de Gestión Ancho de Banda basado en Subred

14.4.3 Ejemplo Gestión de Ancho de Banda basado en Aplicación y Subred

El siguiente ejemplo define las clases en base a subredes de LAN y a aplicaciones.

Tabla 14-1 Ejemplo de Gestión Ancho de Banda basado en Aplicación y Subred

TIPO DE TRÁFICO	DESDE SUBRED A	DESDE SUBRED B
VoIP	64kbps	64kbps
Web	64kbps	64kbps
FTP	64kbps	64kbps
E-mail	64kbps	64kbps
Video	64kbps	64kbps

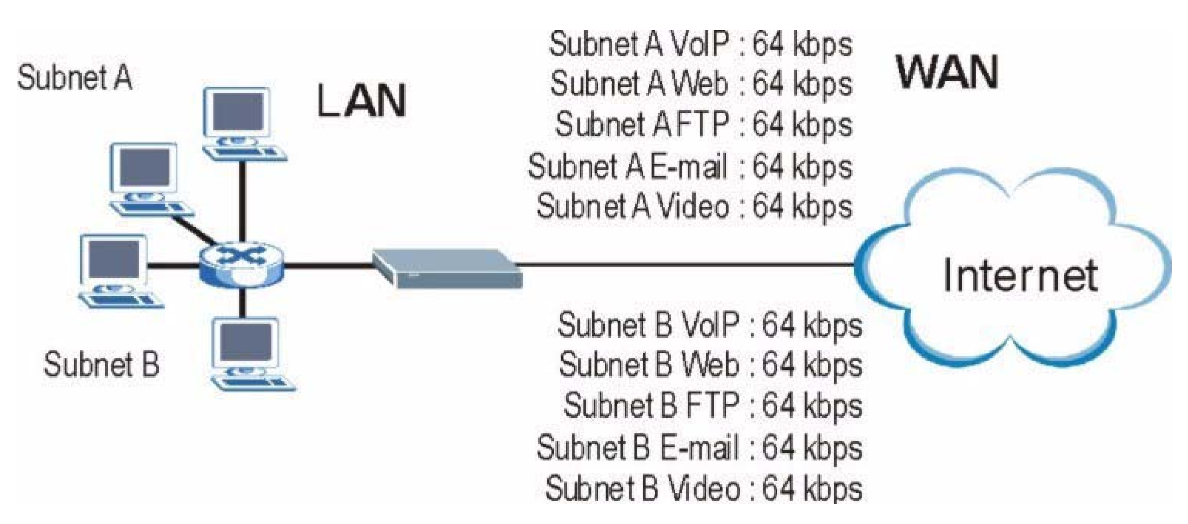


Figura 14-3 Ejemplo de Gestión Ancho de Banda basado en Aplicación y Subred

14.5 Programador

El programador divide el ancho de banda disponible en el interfaz entre las diferentes clases configuradas. El IAD soporta dos tipos de programadores : equitativo (fairness-based) y prioritario (priority-based).

14.5.1 Programador prioritario (priority-based)

Con el programador prioritario, el IAD asigna el tráfico en función de la prioridad definida a las clases. Es recomendable asignar una prioridad más alta a las aplicaciones de tiempo real (tales como audio o video) para asegurar un funcionamiento lo más adecuado posible.

14.5.2 Programador equitativo (fairness-based)

El IAD divide el ancho de banda de forma equitativa entre todas las clases definidas; lo que previene que una única clase acapare el ancho de banda de todo el interfaz.

14.6 Maximización del Uso del Ancho de Banda

La opción para maximizar el ancho de banda (consultar sección 14.7.2) permite al IAD dividir cualquier ancho de banda disponible en el interfaz (incluyendo el ancho de banda no reservado así como el ancho reservado no utilizado por las clases) entre las clases que requiran mayor cantidad de ancho de banda.

Cuando se habilita esta opción, el router en primer lugar asegura que cada clase recibe el ancho de banda reservado. Y adicionalmente, el IAD divide el ancho de banda disponible en la interfaz dependiendo de cuántas clases requieran más ancho de banda y de sus niveles de prioridad. Cuando únicamente una clase requiere más ancho de banda, el IAD asigna el ancho de banda disponible a esta clase.

Cuando existen muchas clases que requiren mayor ancho de banda, el IAD asignará en primer lugar el ancho de banda disponible a las clases más prioritarias (tanto como necesiten, siempre que exista ancho de bnada suficiente), y a continuación a las clases menos prioritarias si todavía queda ancho de banda. El IAD distribuye el ancho de banda disponible de forma equitativa entre todas las clases con el mismo nivel de prioridad.

14.6.1 Reserva de Ancho de Banda para Tráfico no Clasificado

Llevar a cabo los siguientes tres pasos para configurar el IAD con un cierto ancho de banda para tráfico que no está definido por ninguno de los filtros definidos.

1.- Dejar parte del ancho de banda saliente del interfaz sin reservar

2.- No habilitar la opción **Maximize Bandwidth Usage** en el interfaz

3.- No habilitar el préstamo de ancho de banda en las clases que tienen a la clase raíz como clase padre (consultar sección 14.7)

14.6.2 Ejemplo de Maximización del Ancho de Banda

Aquí se muestra un ejemplo en el que se maximiza el uso del ancho de banda en un interfaz. La primera figura muestra el ancho de banda y la prioridad de cada clase. Las clases están definidas en base a la información de subred. El interfaz está configurado a 10Mbps. Cada subred tiene asignados 2Mbps. El tráfico no reservado de 2Mbps permite que el tráfico no definido por ninguno de los filtros pueda salir al exterior cuando no se encuentra selecciona la opción de Maximización del Ancho de Banda.

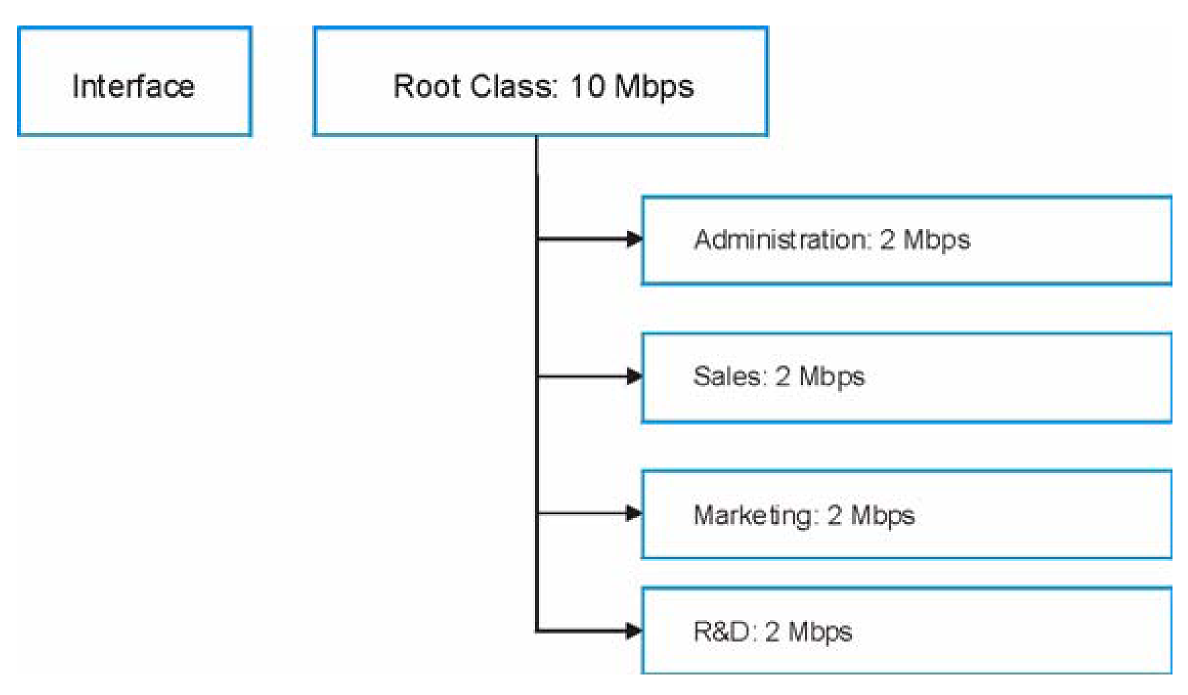


Figura 14-4 Ejemplo Reserva Ancho de Banda

La siguiente figura muestra el uso del ancho de banda con la opción de maximización del uso del ancho de banda habilitado. El IAD divide los 2Mbps no asignados entre las clases que requiren mayor ancho de banda. Si el departamento de Administración únicamente utiliza 1Mbps del ancho reservado de 2Mbps, el IAD divide el ancho de banda remanente de 1Mbps entre las clases que puedan necesitarlo. Además, el IAD divide el ancho de banda total de 3Mpbs no utilizado entre las clases que lo requieren.

En este caso, suponemos que todas las clases excepto la clase Administración necesitan mayor ancho de banda.

- Cada clase utiliza el ancho de banda que tienen asignado. La clase Administración únicamente utiliza 1Mbps de los 2Mbps que tiene asignados.
- Sales y Marketing son las primeras en obtener ancho de banda adicional puesto que son las que tienen el nivel de prioridad más alto (6). Si cada una requiere 1.5Mbps o mayor cantidad de ancho de banda, el IAD dividirá los 3Mbps sin utilizar de forma equitativa entre los departamentos de Sales y Marketing (1.5Mbps para cada uno) dado que ambos tienen el nivel de prioridad más alto.

- El departamento de R&D necesita mayor ancho de banda pero únicamente puede utilizar los 2Mbps que tiene asignados puesto que todo el ancho de banda no utilizado ha sido asignado a las clases más prioritarias.
- El IAD no enviará ningún tipo de tráfico no definido en estos filtros dado que todo el ancho de banda no asignado ha sido utilizado por clases que lo han solicitado.

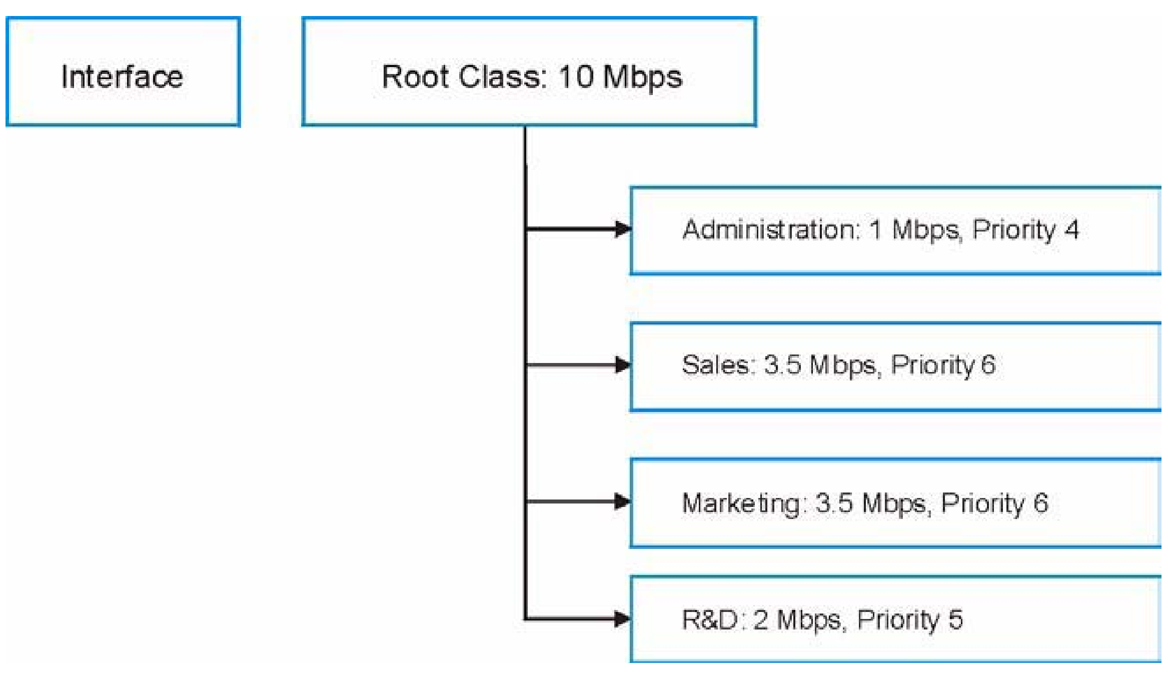


Figura 14-5 Ejemplo de Maximización de Uso del Ancho de Banda

14.7 Préstamo de Ancho de Banda

El préstamo de ancho de banda permite a las clases el solicitar ancho de banda no solicitado por las clases parentales, asimismo al maximizar el uso del ancho de banda permite a las clases el solicitar el uso de ancho de banda no utilizado o no reservado en el interfaz completo.

El ancho de banda no utilizado por una clase es asignado a las clases-hijas que lo soliciten en función del nivel de prioridad. Una clase-hija también puede tomar prestado ancho de banda de una clase de nivel superior si la clase parental de esta clase-hija también está configurada para tomar prestado ancho de banda de su clase superior. Esto puede realizarse para todos los niveles de clases que se encuentren configurados.

El total del ancho de banda reservado para las clases-hijas no puede exceder del ancho de banda reservado en la clase raíz. El IAD utiliza el programador para dividir el ancho de banda no utilizado por la clase parental entre las clases-hijas.

14.7.1 Ejemplo Préstamos de Ancho de Banda

Aquí se muestra un ejemplo de la gestión de ancho de banda con clases configuradas para el préstamo de ancho de banda. Las clases están configuradas en base a departamentos e individuos dentro de ciertos departamentos.

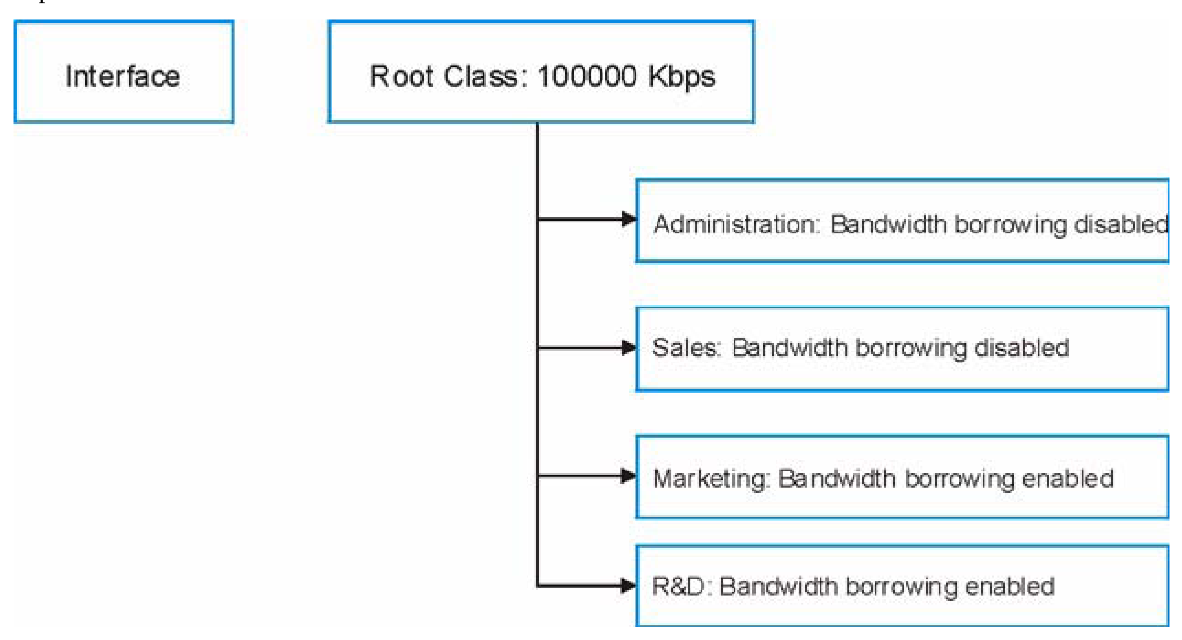


Figura 14-6 Ejemplo Préstamo Ancho de Banda

- Las clases Administración y Sales no pueden tomar prestado ancho de banda no utilizado por la clase raíz dado que dichas clases tienen la funcionalidad del préstamo de ancho de banda deshabilitada.
- Las clases Marketing y R&D podrán tomar prestado ancho de banda no utilizado por la clase raíz dado que ambos sí que disponen de la funcionalidad de préstamo de ancho de banda habilitado.

14.7.2 Maximización del Uso de Ancho de Banda con Préstamo

Si se configuran tanto la maximización del uso del ancho de banda (en un interfaz) así como el préstamo del ancho de banda (en clases individuales), el IAD funcionará como se indica a continuación.

1.- El IAD envía el tráfico en función del ancho de banda reservado para cada clase

2.- El IAD asigna el ancho de banda no utilizado por una clase-parental a sus clases-hijas que necesitan más ancho de banda que la que en principio tienen asignada y disponen de la funcionalidad del préstamo activada. El IAD dará mayor prioridad a las clases-hijas de mayor nivel de prioridad y tratará a las clases de la misma prioridad de forma equitativa.

3.- El IAD asignará cualquier ancho de banda no utilizado o no reservado en la interfaz a cualquier clase que pueda requerirlo. El IAD asigna el ancho restante a las clases con mayor nivel de prioridad en primer lugar y de forma equitativa a las clases con idéntico nivel de prioridad.

4.- El IAD asignará cualquier ancho de banda no reservado al tráfico que no coincida con ninguna de las clases definidas.

14.8 Configuración Gestión Ancho de Banda

Pulse sobre **Media Bandwidth Management**, a continuación **Summary** para abrir la siguiente pantalla.

Habilitar la gestión de ancho de banda en el interfaz y asignar el máximo ancho de banda permitido para este interfaz.

Media Bandwidth Management - Summary

BW Manager manages the bandwidth of traffic flowing out of router on the specific interface. BW Manager can be switched on/off independently for each interface.

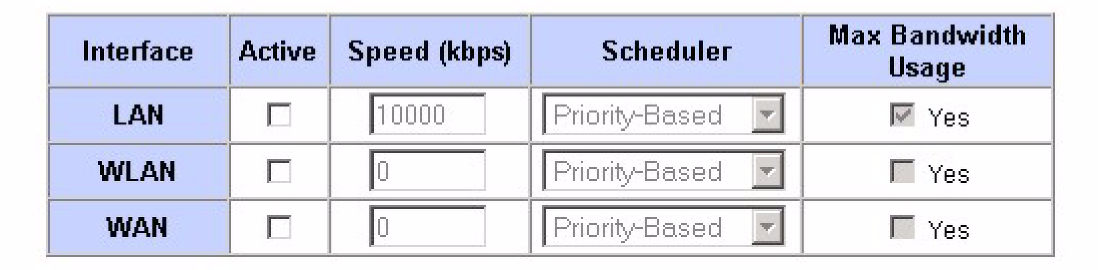




Figura 14-7 Configuración Gestión de Ancho de Banda

La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 14-2 Configuración Gestión de Ancho de Banda

ETIQUETA	DESCRIPCIÓN
LAN WLAN WAN	Estos campos de sólo lectura representan el interfaz físico
Active	Seleccione la casilla de un interfaz para habilitar la gestión de ancho de banda en un interfaz. La gestión de ancho de banda se aplica a todo el tráfico saliente del router a través del interfaz, independientemente de la origen del tráfico. La redirección de tráfico o el IP Alias pueden originar que el tráfico LAN-to-LAN pase a través del router y pueda ser gestionado por esta funcionalidad. La gestión del ancho de banda controla el tráfico saliente de un interfaz, no el entrante. Para limitar el ancho de banda de descarga en los usuarios LAN, configurar la gestión de ancho de banda en la LAN. Así como para limitar el ancho de banda en

	el interfaz inalámbrico, configurar la gestión de ancho de banda para el mismo.
Speed (kbps)	Introduzca la cantidad de ancho de banda reservada para el interfaz para el que desea aplicar esta gestión. Esto aparece como el ancho de banda reservado para el interfaz. La recomendación es configurar esta velocidad de manera que coincida con la velocidad de la conexión que el interfaz puede manejar.
Scheduler	Seleccione **Priority-based** o **Fairness-based** de la lista desplegable para control el flujo de tráfico. Seleccione **Priority-based** para dar mayor preferencia a las clases con mayor prioridad. Seleccione **Fairness-based** para tratar todas las clases de forma equitativa.
Max. Bandwidth Usage	Seleccione esta casilla para que el IAD divida todo el tráfico no reservado y/o no utilizado entre las clases que puedan requerirlo. No seleccione esta casilla si desea reservar cierto ancho de banda para tráfico que no coincida con las clases definidas o se desee limitar la velocidad del interfaz
Back	Pulse **Back** para volver a la pantalla anterior
Apply	Pulse **Apply** para guardar los cambios
Cancel	Pulse **Cancel** para volver a configurar la pantalla de nuevo

14.9 Configuración de Clases

La pantalla de la configuración de clases muestra las clases configuradas en cada interfaz. Seleccione un interfaz y pulse sobre los botones para llevar a cabo las acciones descritas a continuación. Pulse sobre “+” para expandir el árbol de clases y pulse sobre “-“ para comprimir el árbol de clases. Cada interfaz tendrá una clase raíz permanente. El ancho de banda de la clase raíz será igual a la velocidad configurada en el interfaz (ver sección 14.8). Configure las clases-hijas para la clase raíz.

Para añadir o eliminar una clase-hija en un interfaz, pulse sobre Media Bandwidth Management, a continuación Class Setup. Aparecerá la siguiente pantalla.

El siguiente ejemplo reserva 10Mbps de ancho de banda para tráfico que no ha sido definido por ninguna de las clases. Las clases Administración y Sales tienen un ancho de banda asignado superior a la suma total del ancho asignado a sus clases-hijas. Las clases-hijas pueden pedir prestado ancho de banda dado que tienen activada dicha funcionalidad.

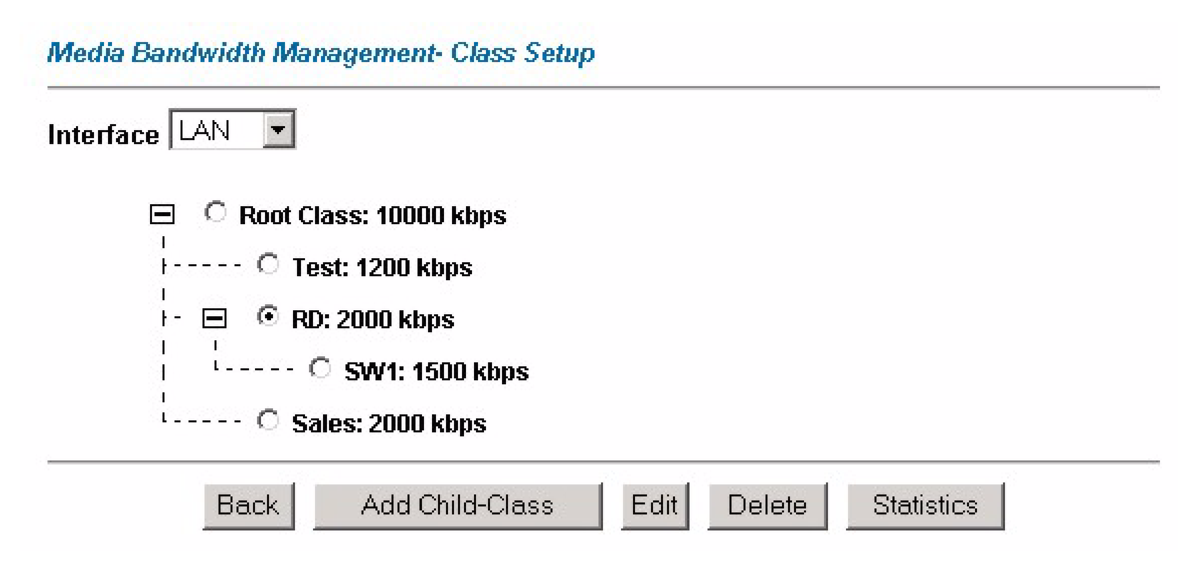


Figura 14-8 Gestión de Ancho de Banda : Configuración de Clases

La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 14-3 Gestión de Ancho de Banda : Configuración de Clases

ETIQUETA	DESCRIPCIÓN
Interface	Seleccione un interfaz de la lista desplegable para el que se desean configurar las clases
Back	Pulse **Back** para volver a la pantalla **Media Bandwidth Management**.
Add Child-Class	Pulse **Add Child-Class** para añadir una subclase
Edit	Pulse **Edit** para configurar la clase seleccionada. No es posible editar la clase raiz.
Delete	Pulse **Delete** para eliminar la clase y todas sus clases-hijas. No es posible eliminar la clase raíz.
Statistics	Pulse **Statistics** para mostrar el estado de la clase seleccionada.

14.9.1 Configuración de Clases de Gestión de Ancho de Banda

La configuración de la clase se realiza en la pantalla **Class Configuration**. Es necesario en la pantalla **Media Bandwidth Management – Summary** el habilitar la gestión de ancho de banda en el interfaz antes de configurar las clases para el mismo.

Para añadir una clase-hija, pulse sobre **Media Bandwidth Management**, a continuación sobre **Class Setup**. Pulse sobre el botón **Add Child-Class** para abrir la siguiente pantalla.

Media Bandwidth Management- Class Configuration

Class Name lan-2.2
BW Budget 0 (kbps)
Priority 3 (0-7)
Borrow bandwidth from parent class

Bandwidth Filter
Active
Service None
Destination IP Address
Destination Subnet Mask
Destination Port 0
Source IP Address
Source Subnet Mask
Source Port 0
Protocol ID 0

Back Apply Cancel

Figura 14-9 Configuración de una clase

La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 14-4 Configuración de una clase

ETIQUETA	DESCRIPCIÓN
Class Name	Utilice el nombre que se genera automáticamente o introduzca un nombre descriptivo de hasta 20 caracteres
BW Budget (kbps)	Especifique el máximo ancho de banda reservado para esta clase.
Priority	Introduzca un número entre 0 y 7 para configurar la prioridad de la clase. Mientras mayor es el número, más alta es la prioridad. El valor por defecto es 3.
Borrow bandwidth from parent class	Seleccione esta opción para permitir que la clase-hija pueda pedir prestado ancho de banda de su clase parental si ésta no está utilizando todo su ancho de banda. El préstamo del ancho de banda está gobernado por la prioridad de las clases-hijas. Esto es, una clase-hija con la máxima prioridad (7) será la primera en recibir prestado ancho de banda de su clase parental. No seleccione esta casilla en las clases directamente dependientes de la clase raiz si desea dejar cierto ancho de banda disponible para otro tipo de tráfico que no coincida con ninguna de las clases configuradas.
Bandwidth Filter El IAD utiliza el filtro para identificar el tráfico que pertenece a una clase.	
Active	Seleccione esta casilla para que el IAD utilice este filtro cuando se habilite la funcionalidad de gestión del ancho de banda.
Service	Es posible seleccionar uno de los servicios predefinidos en lugar de configurar los campos **Destination Port, Source Port** y **Protocol ID**. SIP (Session Initiation Protocol) es un protocolo de señalización utilizado en la telefonía Internet, mensajería instantánea y otras aplicaciones de VoIP. Seleccione **SIP** de la lista desplegable para asociar el filtro para tráfico SIP. File Transfer Protocol (FTP) es un protocolo de transferencia de ficheros que opera sobre redes TCP/IP. Un sistema ejecutando un servidor FTP acepta los comandos recibidos de un sistema ejecutando un cliente FTP. El servicio permite a los usuarios enviar comandos al servidor para cargar o descargar ficheros. Seleccione **FTP** de la lista desplegable para asociar el filtro para tráfico FTP. H.323 es un protocolo estándar de teleconferencia que proporciona conferencia para audio, datos y voz. Seleccione **H.323** de la lista desplegable para asociar el

	filtro al tráfico que utilice H.323. Cuando se seleccione None, la clase se aplica a todos los servicios a menos que se especifique uno mediante la configuración de los campos **Destination Port, Source Port** y **Protocol ID**.
Destination IP Address	Introduzca la dirección IP de destino. Una dirección en blanco indica cualquier dirección IP de destino.
Destination Subnet Mask	Introduzca la máscara de subred de destino. Este campo estará N/A si no se especifica una dirección IP de destino.
Destination Port	Introduzca el puerto de destino. Un puerto de destino en blanco indica cualquier puerto de destino.
Source IP Address	Introduzca la dirección IP origen. Una dirección en blanco indica cualquier dirección IP origen.
Source Subnet Mask	Introduzca la máscara de subred origen. Este campo estará N/A si no se especifica una dirección IP origen.
Source Port	Introduzca el puerto origen. Un puerto origen en blanco indica cualquier puerto origen.
Protocol ID	Introduzca el número de protocolo (tipo de servicio), por ejemplo : 1 para ICMP, 6 para TCP o 17 para UDP. Un valor en blanco indica cualquier protocolo.
Back	Pulse **Back** para volver a la pantalla anterior **Media Bandwidth Management**.
Apply	Pulse **Apply** para guardar los cambios
Cancel	Pulse **Cancel** para volver a configurar la pantalla de nuevo

Tabla 14-5 Servicios y Números de Puerto

SERVICIOS	**NÚMERO DE PUERTO**
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79

HTTP (Hyper Text Transfer Protocol o WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP Trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

14.9.2 Estadísticas Gestión de Ancho de Banda

Utilice la pantalla de **Media Bandwidth Management Statistics** para visualizar la información de rendimiento de la red. Pulse sobre el botón **Statistics** en la pantalla **Class Setup** para abrir la pantalla **Statistics**.

Class Name: Root Class **Budget: 10000 (kbps)**

Tx Packets	Tx Bytes	Dropped Packets	Dropped Bytes
1089	805376	0	0

Bandwidth Statistics for the Past 8 Seconds

t-8	t-7	t-6	t-5	t-4	t-3	t-2	t-1
0	0	0	33	52	58	86	62



Figura 14-10 Estadísticas Gestión Ancho de Banda

La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 14-6 Estadísticas Gestión Ancho de Banda

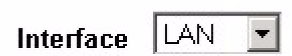
ETIQUETA	DESCRIPCIÓN
Class Name	Este campo muestra el nombre de la clase cuyas estadísticas se muestran

Budget (kbps)	Este campo muestra la cantidad de ancho de banda reservado para la clase
Tx Packets	Este campo muestra el número total de paquetes transmitidos
Tx Bytes	Este campo muestra el número total de bytes transmitidos
Dropped Packets	Este campo muestra el número total de paquetes descartados
Dropped Bytes	Este campo muestra el número total de paquetes descartados
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
Este campo muestra las estadísticas de ancho de banda (kbps) durante los últimos 8 segundos. For ejemplo, t-1 indica que ocurrió hace 1 segundo	
Update Period (seconds)	Introduzca el intervalo en segundos que define cada cuantos segundos se refrescará la información
Set Interval	Pulse **Set Interval** para aplicar el nuevo valor del periodo introducido en el campo **Update Period**.
Stop Update	Pulse **Stop Update** para detener el refresco de estadísticas en la pantalla del navegador.
Clear Counter	Pulse **Clear Counter** para borrar todas las estadísticas.

14.10 Monitor de Ancho de Banda

Para visualizar tanto la utilización como el ancho de banda reservado para cada interfaz, pulse sobre **Media Bandwidth Management**, y a continuación **Monitor**. La pantalla que aparece será la siguiente.

Media Bandwidth Management- Monitor



Class Name	Budget (kbps)	Current Usage (kbps)
Root Class	10000	59
Test	1200	0
RD	2000	0
SW1	1500	0
Sales	2000	0



Figura 14-11 Gestión de Ancho de Banda : Monitor

La siguiente tabla describe las etiquetas de esta pantalla.

Tabla 14-7 Gestión de Ancho de Banda : Monitor

ETIQUETA	DESCRIPCIÓN
Interface	Seleccione el interfaz de la lista desplegable para visualizar el uso de ancho de banda de sus clases
Class Name	Este campo muestra el nombre de la clase
Budget (kbps)	Este campo muestra la cantidad de ancho de banda asignada a esta clase
Current Usage (kbps)	Este campo muestra la cantidad de ancho de banda que está utilizando cada clase
Back	Pulse **Back** para volver a la pantalla **Media Bandwidth Management**
Refresh	Pulse **Refresh** para actualizar la página

Capítulo 15
Mantenimiento

Este capítulo muestra la información del sistema tales como firmware ZyNOS, direcciones IP de los puertos y estádisiticas de tráfico en los puertos.

15.1 Descripción de Mantenimiento

Las ventanas de mantenimiento ayudan a ver información de sistema, actualización de firmware, gestionar la configuración y reiniciar su Prestige.

15.2 Pantalla Estado del Sistema

Pulse **Estado del Sistema (System Status)** para abrir la siguiente pantalla, donde podrá monitorizar el estado de su Prestige. Hacer notar que estos campos son de SOLO LECTURA y únicamente para propósitos de diagnóstico.

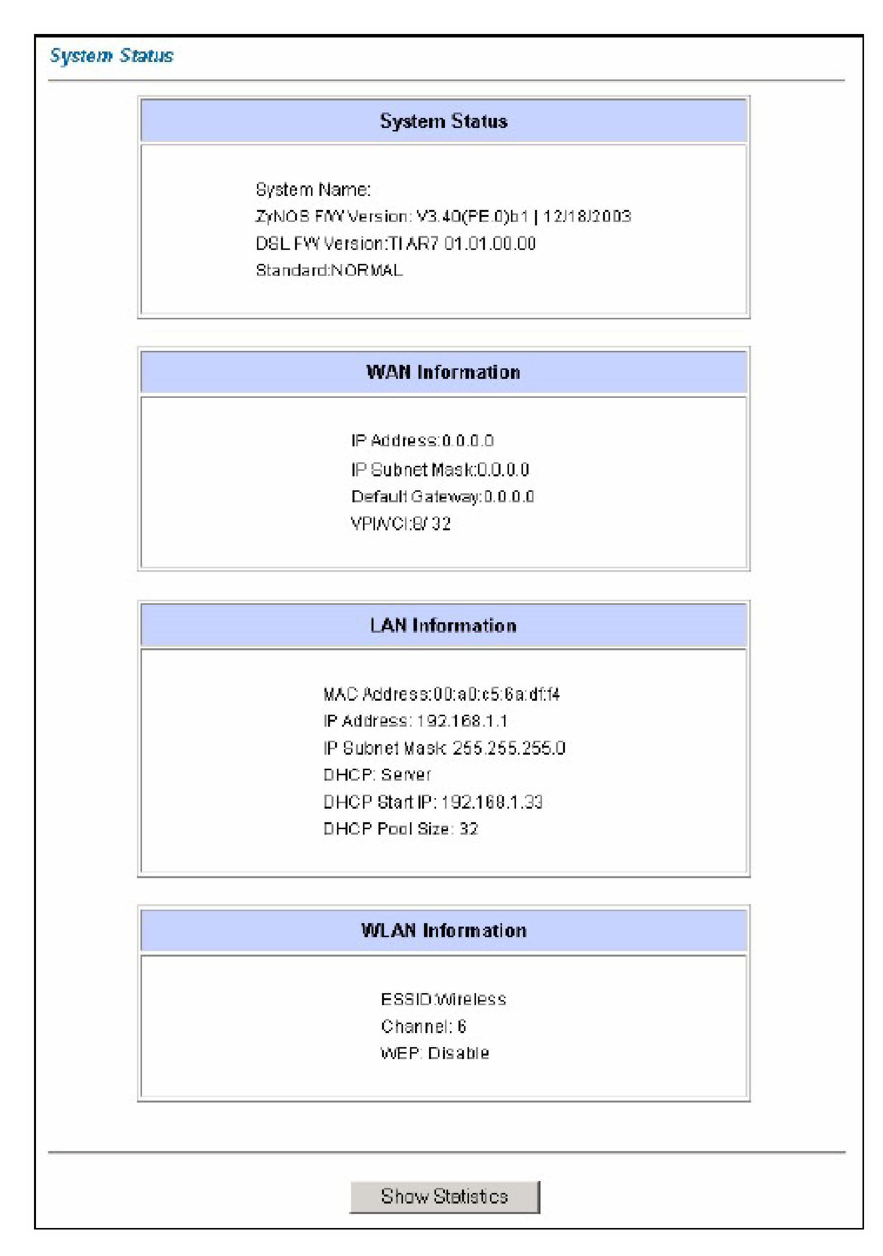


Figura 15-1 Estado del Sistema

La siguiente tabla describe los campos de esta pantalla.

Tabla 15-1 Estado del Sistema

ETIQUETA	DESCRIPCIÓN
System Status	
System Name	Éste es el nombre de su Prestige. Únicamente para motivos de identificación.
ZyNOS Firmware Version	Ésta es la versión firmware del ZyNOS y la fecha de creación. ZyNOS es el Sistema Operativo propietario de ZyXEL.
DSL FW Version	Ésta es la version firmware DSL asociada con su Prestige.
Standard	Éste es el estándar que su Prestige utiliza.
WAN Information	
IP Address	Ésta es la dirección IP del puerto WAN.
IP Subnet Mask	Ésta es la máscara de subred del puerto WAN.
Default Gateway	Ésta será la puerta de enlace predeterminada, si se aplica.
VPI/VCI	Éste es el Identificador de Trayecto Virtual y el Identificador de Canal Virtual.
LAN Information	
MAC Address	Ésta es la dirección MAC o la dirección Ethernet única para su Prestige.
IP Address	Ésta es la dirección IP del puerto LAN.
IP Subnet Mask	Ésta será la máscara de subred del puerto LAN.
DHCP	Esto indica el rol del puerto LAN **– Server , Relay** (no todos los modelos) o **None**.
DHCP Start IP	Ésta es la primera dirección contigua del conjunto de direcciones IP.
DHCP Pool Size	Éste es el número de direcciones IP que contiene el conjunto.
WLAN Information	
ESSID	Éste es el nombre descriptivo utilizado para identificar al Prestige en la red wireless LAN.
Channel	Éste es el número de canal utilizado por el Prestige.
WEP	Esto muestra el estado de la encriptación WEP.

Show Statistics	Pulse sobre **Show Statistics** para visualizar las estadísticas de funcionamiento tales como el número de paquetes enviados y recibidos por cada puerto.

15.2.1 Estadísticas de Sistema

Pulse sobre **Mostrar Estadísticas** - **Show Statistics** en la pantalla de **Estado del Sistema** - **System Status** para abrir la siguiente pantalla. La información de sólo-lectura incluye el estado de los puertos y las estadísticas específicas de los paquetes. También proporciona el tiempo que lleva el sistema levantado así como el tiempo de refresco de la información. El campo del **Perido de Refresco (Poll Interval)** es configurable.

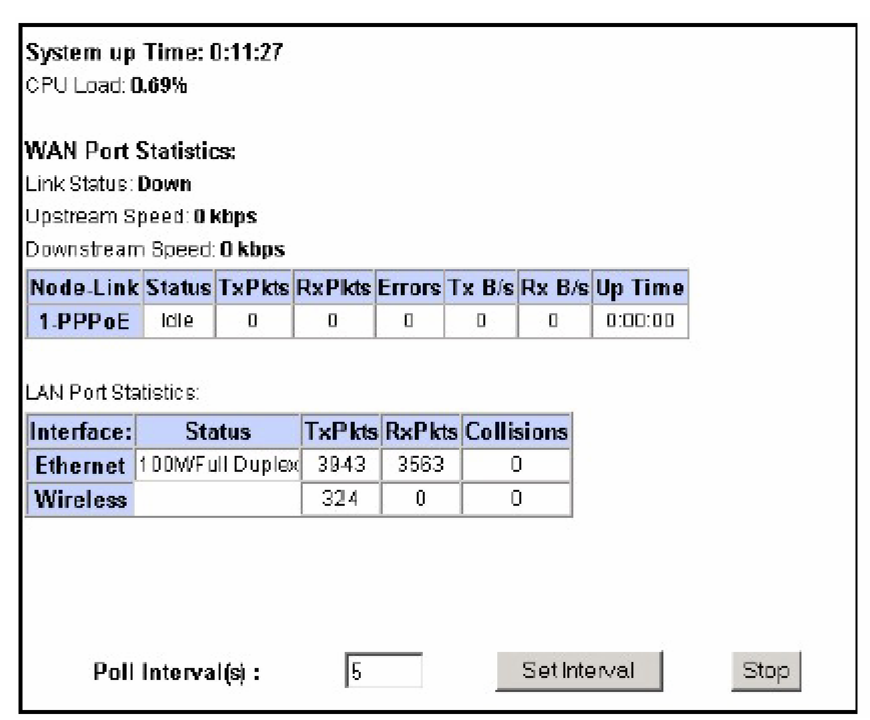


Figura 15-2 Estado del Sistema : Visualización de Estadísticas

La siguiente tabla describe los campos de esta pantalla.

Tabla 15-2 Estado del Sistema : Visualización de Estadísticas

ETIQUETA	DESCRIPCIÓN
System up Time	Éste es el periodo de tiempo que lleva el sistema levantado.
CPU Load	Este campo especifica el porcentaje de CPU utilizado.
LAN or WAN Port Statistics	Éste es el puerto WAN o LAN.
Link Status	Éste es el estado del enlace WAN.
Upstream Speed	Ésta es la velocidad del enlace de subida.
Downstream Speed	Ésta es la velocidad del enlace de bajada.
Node-Link	Este campo muestra el número del nodo remoto y el tipo de enlace. Los tipos de enlaces son PPPoA, ENET, RFC 1483 y PPPoE.
Interface	Esta campo muestra el tipo de puerto.
Status	Para el puerto WAN, muestra la velocidad del puerto y el modo duplex si se está utilizando encapsulación Ethernet; y **down** (la línea está caída), **idle** (línea ppp sin negociar), **dial** (comienzo del marcado de la llamada) y **drop** (tirando la llamada) si se está utilizando la encapsulación PPPoE. Para el puerto LAN, mostrará la velocidad del puerto y el modo duplex.
TxPkts	Este campo muestra el número de paquetes transmitidos por este puerto.
RxPkts	Este campo muestra el número de paquetes recibidos por este puerto.
Errors	Este campo muestra el número de paquetes de error en este puerto.
Tx B/s	Este campo muestra el número de bytes transmitidos en el último segundo.
Rx B/s	Este campo muestra el número de bytes recibidos en el último segundo.
Up Time	Este campo indica el tiempo que ha transcurrido desde que este puerto se levantó.
Collisions	Éste es el número de colisiones en este puerto.
Poll Interval (s)	Introduzca el intervalo de refresco de estadísticas del navegador.
Set Interval	Pulse este botón para aplicar el nuevo periodo de refresco introducido en el campo **Poll Interval** anterior.
Stop	Pulse este botón para detener el refresco de las estadísticas del sistema.

15.3 Pantalla Tabla DHCP

DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuración de Host Dinámica, RFC 2131 y RFC2132) permite a los clientes obtener la configuración TCP/IP al iniciar desde un servidor. Puede configurar su Prestige como servidor DHCP o deshabilitar. Cuando está configurado como servidor, el Prestige proporciona la configuración TCP/IP a los clientes. Si está configurado a **None (No),** el servicio DHCP está deshabilitado y deberá disponer de otro servidor DHCP en la LAN, o configurar manualmente los parámetros en los ordenadores.

Pulse **Maintenance**, y a continuación la pestaña **DHCP Table**. La información de sólo-lectura indica el estado DHCP. La tabla DHCP muestra la información DHCP de clientes actual (incluyendo la **Dirección IP, Host Name** y **Dirección MAC**) de todos los clientes de red utilizando el servidor DHCP.

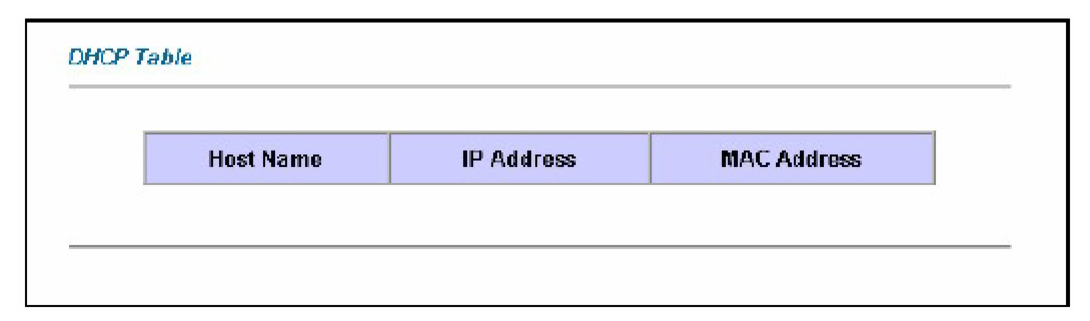


Figura 15-3 Tabla DHCP

La siguiente tabla describe los campos de esta pantalla.

Tabla 15-3 Tabla DHCP

ETIQUETA	DESCRIPCIÓN
Host Name	Éste es el nombre de la máquina.
IP Address	Este campo muestra la dirección IP relativa al nombre de máquina anterior.
MAC Address	Este campo muestra la dirección MAC del ordenador con el nombre de máquina mostrado. Cada dispositivo Ethernet tiene una dirección MAC única. La dirección MAC asignada en fábrica consiste en seis pares de caracteres hexadecimales, por ejemplo, 00:A0:C5:00:00:02

15.4 Pantalla Wireless

La pantalla de solo-lectura muestra información sobre la interfaz Wireless LAN del Prestige.

15.4.1 Lista de Asociación

Este pantalla muestra la dirección o direcciones MAC de las estaciones wireless que están actualmente conectadas en la red. Pulse sobre Wireless LAN y a continuación sobre Association List para abrir la siguiente pantalla.

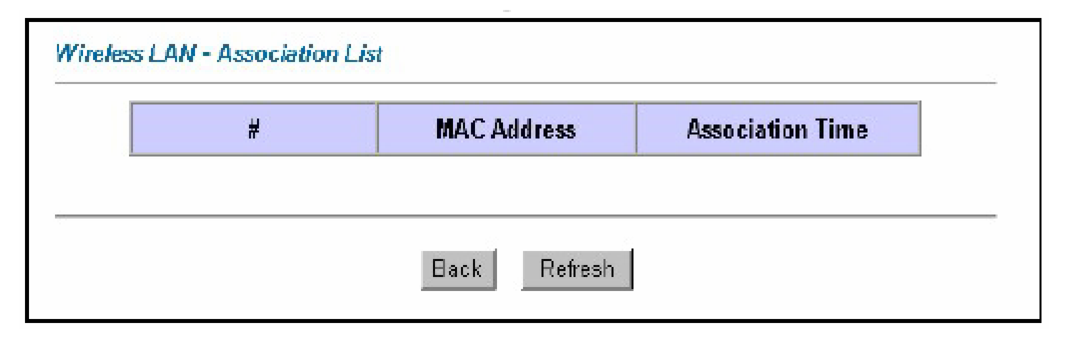


Figura 15-4 Lista de Asociación

La siguiente tabla describe los campos de esta pantalla.

Tabla 15-4 Lista de Asociación

ETIQUETA	DESCRIPCIÓN
#	Éste es el índice de una estación wireless asociada.
MAC Address	Este campo muestra la dirección MAC de la estación wireless asociada. Cada dispositivo Ethernet tiene una dirección MAC única. La dirección MAC es asignada en fábrica y consiste en seis pares de caracteres hexadecimales, por ejemplo, 00:A0:C5:00:00:02.
Association Time	Este campo muestra el tiempo que una estación wireless lleva asociada al Prestige.
Back	Pulse **Back** para volver a la pantalla previa.
Refresh	Pulse **Refresh** para renovar la información de la tabla.

15.5 Pantallas de Diagnóstico

Estas pantallas de sólo-lectura muestra información para ayudarle a identificar problemas con el Prestige.

15.5.1 Pantalla General de Diagnóstico

Pulse sobre **Diagnostic** y a continuación sobre **General** para abrir la siguiente pantalla.

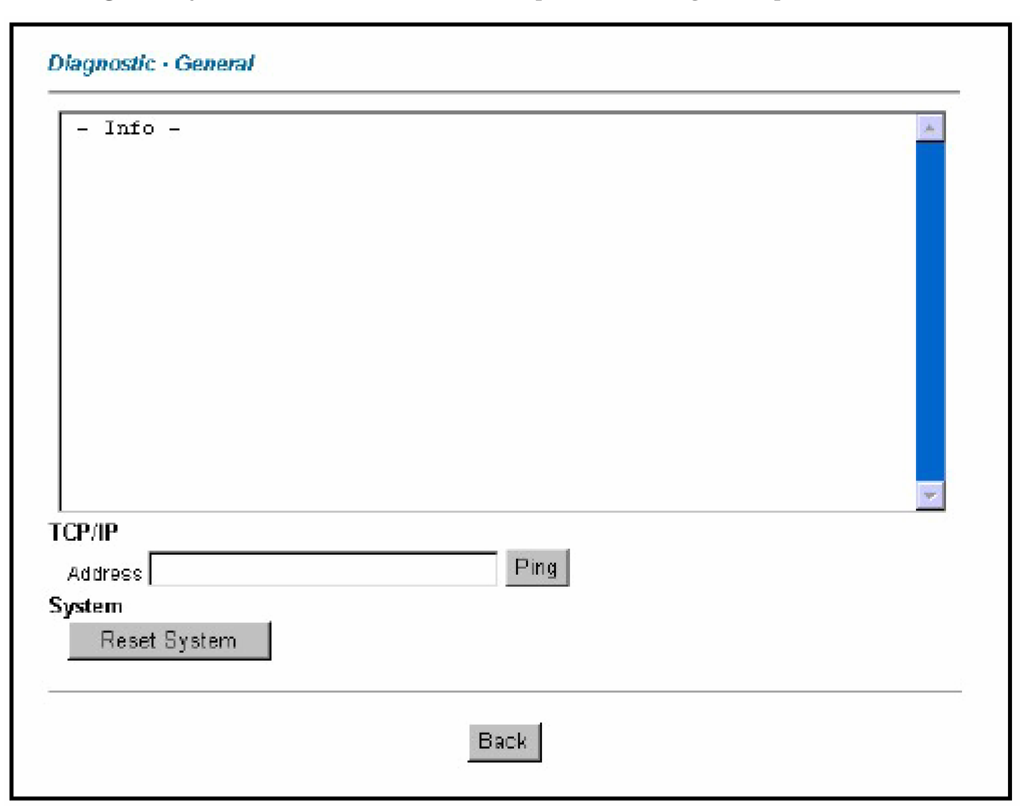


Figura 15-5 Diagnóstico General

La siguiente tabla describe los campos de esta pantalla.

Tabla 15-5 Diagnóstico General

ETIQUETA	DESCRIPCIÓN
TCP/IP Address	Introduzca la dirección IP del ordenador al que se desee hacer ping para comprobar su conexión.
Ping	Pulse este botón para hacer ping a la dirección IP que se haya introducido.
Reset System	Pulse este botón para reiniciar el Prestige. Un cuadro de aviso aparecerá pidiéndole confirmación para el reinicio del sistema. Pulse **OK** para proceder.
Back	Pulse este botón para volver a la pantalla principal de **Diagnóstico (Diagnostic)**.

15.5.2 Pantalla de Diagnóstico de la Línea DSL

Pulse Diagnostic y a continuación DSL Line para abrir la siguiente ventana.



Figura 15-6 Diagnóstico de Línea DSL

La siguiente tabla describe los campos de esta ventana.

Tabla 15-6 Diagnóstico Línea DSL

ETIQUETA	DESCRIPCIÓN
Reset ADSL Line	Pulse este botón para reiniciar la línea ADSL. El línea de texto arriba muestra el progreso y el resultado de esta operación, por ejemplo: “Start to reset ADSL Loading ADSL modem F/W… Reset ADSL Line Successfully!”
ATM Status	Pulse este botón para ver el estado ATM.
ATM Loopback	Pulse este botón para comenzar el test Loopback ATM. Asegúrese que ha configurado

Test	al menos un PVC con los valores adecuados de VPI/VCI antes de llevar a cabo este tests. El Prestige envía un paquete OAM F5 al DSLAM o switch ATM y lo devuelve al Prestige. El test loopback ATM es útil para resolución de problemas con el DSLAM y la red ATM.
Upstream Noise Margin	Pulse este botón para mostrar el margen de ruido en el canal ascendente.
Downstream Noise Margin	Pulse este botón para visualizar el margen de ruido en el canal descendente.
Back	Pulse este botón para volver a la pantalla principal de **Diagnóstico – Diagnostic**.

15.6 Pantalla de Firmware

Podrá encontrar el firmware en la página www.zyxel.com en un fichero con extensión .bin dentro de un fichero comprimido. El proceso de carga utiliza http y puede tardar un par de minutos. Tras la actualización, el sistema se reiniciará. Consulte el capítulo de Firmware y Mantenimiento del Fichero de Configuración en la parte del documento del SMT para actualización de firmware utilizando comandos FTP/TFTP.

Utilizar únicamente firmware para el modelo de dispositivo específico. Consulte la etiqueta en la parte inferior del dispositivo.

Pulse **Firmware** para abrir la siguiente pantalla. Siga las intrucciones en esta pantalla para cargar el firmware al Prestige.

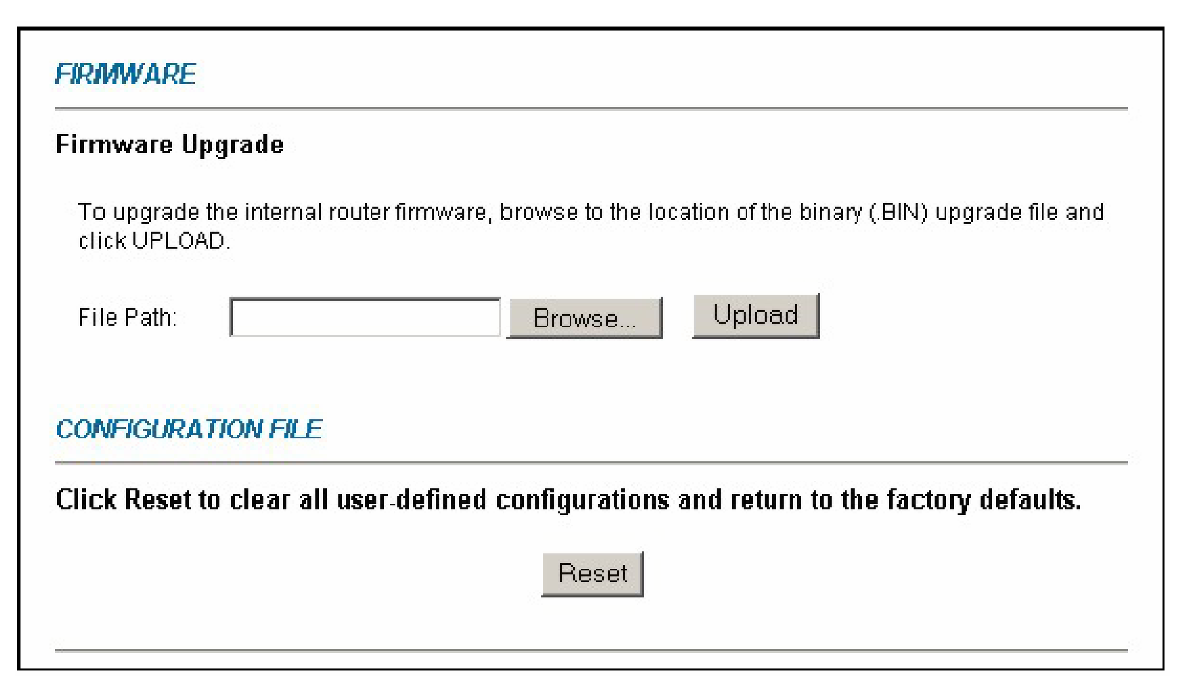


Figura 15-7 Actualización de Firmware

La siguiente tabla describe las etiquetas en esta pantalla.

Tabla 15-7 Actualización de Firmware

ETIQUETA	DESCRIPCIÓN
File Path	Introduzca la localización del fichero que desea subir en el este campo o pulse **Browse**…. para encontrarlo.
Browse…	Pulse **Browse…** para encontrar el fichero .bin que desea cargar. Recuerde que debe descomprimir el fichero zip antes de subirlo.
Upload	Pulse **Upload** para comenzar la actualización. Este proceso puede durar un par de minutos.
Reset	Pulse este botón para borrar toda la configuración de usuario y devolver el Prestige a la configuración por defecto. Consulte la sección acerca de Resetear el Prestige.

No apague el Prestige durante el proceso de actualización de firmware!!!!

Tras visualizar la pantalla de Actualización de Firmware en Proceso (Firmware Upload in Process), espere un par de minutos antes de registrarse nuevamente en el Prestige.

El Prestige se reiniciará automáticamente causando pérdida temporal de la conexión de red. En algunos sistemas operativos podrá aparecerá el siguiente icono en su escritorio.

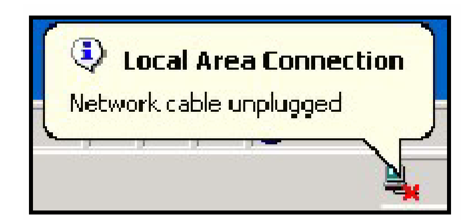


Figura 15-8 Red Temporalmente Desconectada

Tras dos minutos, regístrese nuevamente y compruebe que su nueva versión de firmware aparece en la pantalla de **Estado del Sistema (System Status)**.

Si la actualización no fue satisfactoria, aparecerá la siguiente pantalla. Pulse **Back** para volver a la pantalla de **Firmware.**

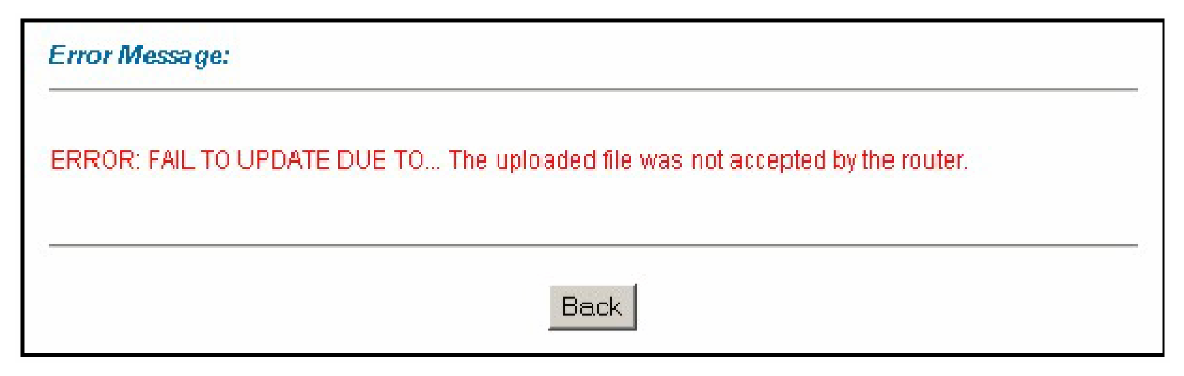


Figura 15-9 Mensaje de Error

Capítulo 16
Introducción al SMT

Este capítulo explica como acceder y navegar por el Terminal de Gestión del Sistema y ofrece una descripción de sus términos.

16.1 Introducción SMT

El SMT del Prestige (System Management Terminal – Terminal de Gestión del Sistema) es un interfaz basado en menús accesible de un emulador de terminal sobre una conexión telnet. Esta capítulo muestra como acceder a los menús SMT a través de Telnet, como navegar a través del SMT y como configurar los diferentes menús.

16.1.1 Procedimiento de Configuración via Telnet

El siguiente procedimiento detalla como hacer telnet al Prestige.

Paso 1. En Windows, pulse sobre **Inicio, Ejecutar** e introduzca “telnet 192.168.1.1” (dirección IP por defecto) y pulse sobre **Aceptar**.

Paso 2. Introduzca “1234” en el campo de **Password**.

Paso 3. Tras introducir la contraseña verá la pantalla del menú principal.

Por favor, tenga en cuenta que si no hay actividad durante más de cinco minutos (temporizador por defecto) tras haberse registrado, el Prestige automáticamente cerrará la sesión. Será necesario volver a registrarse para entrar en el equipo.

16.1.2 Introducir la contraseña

La pantalla de login aparece tras pulsar [INTRO], pidiendo la introducción de la contraseña, como se muestra a continuación.

La primera vez que acceda, introduzca “1234” como la contraseña por defecto. Al teclear la contraseña, en la pantalla aparecerán asteriscos “*” para cada carácter tecleado.

Por favor, tenga en cuenta que si no hay actividad durante más de cinco minutos (temporizador por defecto) tras haberse registrado, el Prestige automáticamente cerrará la sesión. Será necesario volver a registrarse para entrar en el equipo.

```
Enter Password : ****
```

Figura 16-1 Pantalla de login

16.1.3 Descripción del menú SMT

Utilizaremos los menús del P660HW-D1 como ejemplo. Los menús SMT podrán variar ligeramente entre los diferentes modelos de Prestige.

La siguiente figura da una descripción de las diferentes pantallas del menú del Prestige.

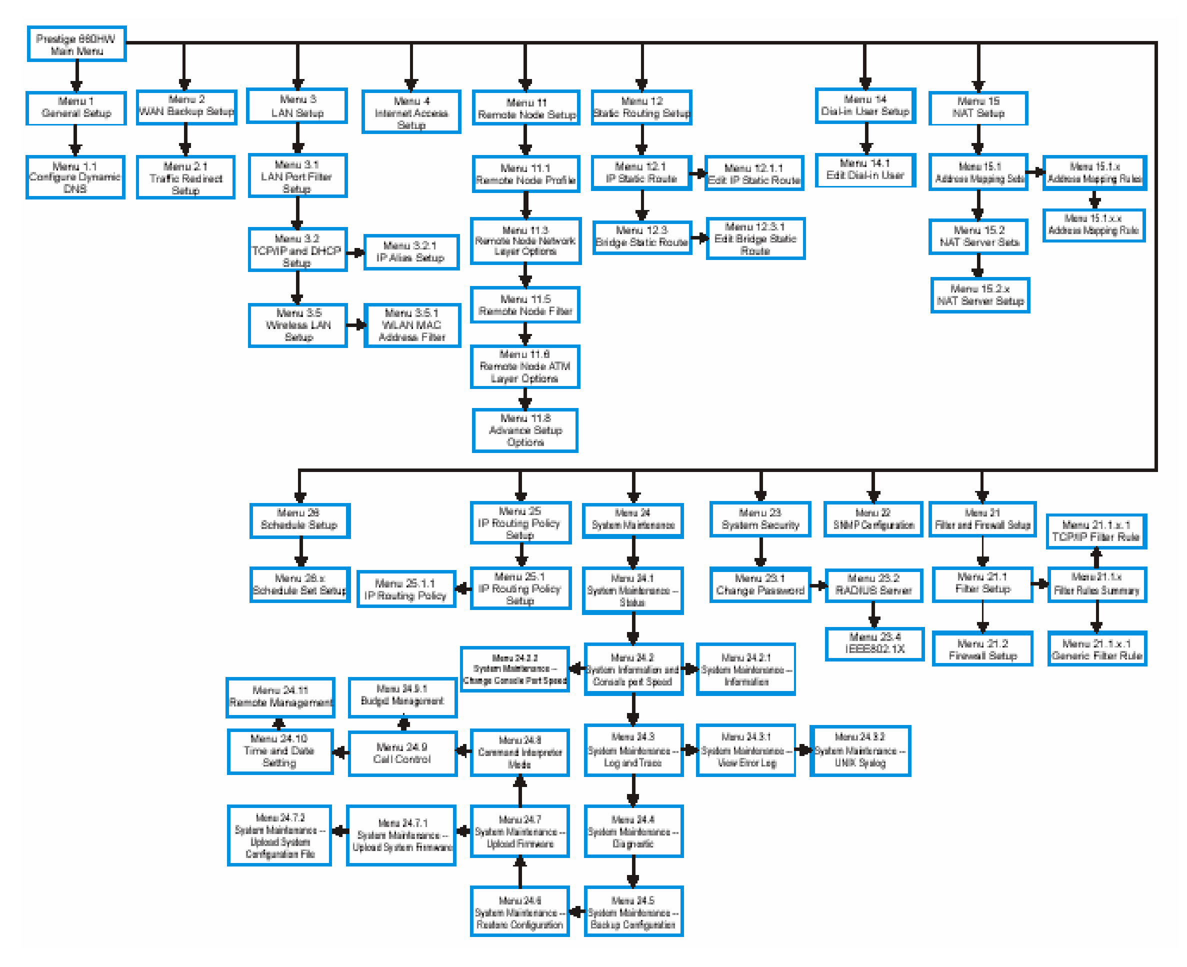


Figura 16-2 Descripción del Menú SMT del P660HW-D1

16.2 Navegando por el interfaz SMT

El SMT es un interfaz utilizado para configurar el Prestige.

Variar operaciones con lo que debe familiarizarse antes de intentar modificar la configuración se listan a continuación.

Tabla 16-1 Comandos Menú Principal

OPERACIÓN	TECLADO	DESCRIPCIÓN
Moverse hacia abajo por el menú	[ENTER]	Para seguir por un submenu, introduzca el número del submenú deseado y presione [ENTER].
Moverse hacia arriva a un menú superior	[ESC]	Presione [ESC] para volver al menú previo.
Moverse hacia un menú “oculto”	Presione [BARRA ESPACIADORA] para cambiar de **No** a **Yes** luego presione [ENTER].	Los campos que empiezan con “Edit” conducen a menús ocultos y por defecto presentan el valor **No**. Presione [BARRA ESPACIADORA] una vez para cambiar de **No** a **Yes**, luego presione [ENTER] para ir al menú “oculto”.
Mover el cursor	[ENTER] o [ARRIBA/ABAJO] cursores	Dentro de un menú presione [ENTER] para moverse al siguiente campo. También puede usar los cursores [ARRIBA/ABAJO] para moverse a los campos anterior y siguiente, respectivamente.
Introducir información	Escriva o presione [BARRA ESPACIADORA]], luego presione [ENTER].	Usted necesita rellenar dos tipos de campos. El primero requiere que introduzca la información apropiada. El segundo le permite seleccionar los valores disponibles presionando [BARRA ESPACIADORA].
Campos requeridos	<? > or **ChangeMe**	Todos los campos con el símbolo <?> deben ser rellenados para poder salvar la nueva configuración. Todos los campos con **ChangeMe** no se deben dejar en blanco para poder guardar la nueva configuración.
Campos N/A	<N/A>	Algunos de los campos en el SMT mostrarán <N/A>. Éste simbolo hace referencia a opciones que no pueden ser aplicadas.
Guardar la configuración	[ENTER]	Guarde los cambios pulsando [INTRO] en la línea con el mensaje “Press ENTER to confirm or ESC to cancel”. Al guardar los cambios volverá en la mayoría de los casos al menú anterior.
Salir del SMT	Teclee 99 y presione [ENTER].	Teclee 99 en el menú principal y presione [ENTER] para salir de la interfaz SMT.

Después de haber introducido la contraseña, aparecerá el menú principal SMT tal y como se muestra a continuación.

```
                  Copyright (c) 1994 - 2006 ZyXEL Communications Corp.

                            P-660HW-D1 Main Menu

   Getting Started                      Advanced Management
     1. General Setup                     21. Filter Set Configuration
     2. WAN Backup Setup                  22. SNMP Configuration
     3. LAN Setup                         23. System Security
     4. Internet Access Setup             24. System Maintenance
                                          25. IP Routing Policy Setup
   Advanced Applications                  26. Schedule Setup
     11. Remote Node Setup
     12. Static Routing Setup
     14. Dial-in User Setup               99. Exit
     15. NAT Setup




                      Enter Menu Selection Number:
```

Figura 16-3 Menú Principal SMT

16.2.1 Resumen de la Interfaz SMT

Tabla 16-2 Resumen Menú Principal

#	TÍTULO DEL MENÚ	DESCRIPCIÓN
1	General Setup	Use este menú para introducir información general.
2	WAN Backup Setup	Utilice este menú para configurar la redirección del tráfico y el dial backup.
3	LAN Setup	Use este menú para configurar su conexión.
4	Internet Access Setup	Rápido y fácil método de configurar su conexión a.
11	Remote Node Setup	Use este menú para configurar el nodo remoto en conexiones LAN-to-LAN, incluyendo conexiones a Internet.
12	Static Routing Setup	Use este menú para configurar rutas estáticas.
15	NAT Setup	Use este menú para especificar servidores internos cuando tenga activada la opción.
21	Filter Setup	Use este menú para configurar filtros.
22	SNMP Configuration	Use este menú para configurar parametros relacionados con el SNMP.

#	TÍTULO DEL MENÚ	DESCRIPCIÓN
23	System Security	Use este menú para configurar la seguridad wireless y modificar la contraseña.
24	System Maintenance	Este menú incluye estado del sistema, diagnosticos, carga de software, etc.
25	IP Routing Policy Setup	Use este menú para configurar su política de enrutado.
26	Schedule Setup	Use este menú para programar llamadas salientes.
99	Exit	Use este menú para salir del SMT y regresar a la pantalla en blanco.

16.3 Modificar la Contraseña del Sistema

Para cambiar la contraseña por defecto de su Prestige siga los siguientes pasos:

Paso 1. Introduzca **23** en el menú principal para mostrar **Menu 23 - System Security** tal como se muestra abajo.

Paso 2. Introduzca 1 para mostrar el **Menu 23.1 – System Security – Change Password** como se indica.

Paso 3. Teclee su contraseña actual en el campo **Old Password**, por ejemplo “1234”, y pulse [INTRO].

```
          Menu 23.1 - System Security - Change Password

            Old Password= ?
            New Password= ?
            Retype to confirm= ?


             Enter here to CONFIRM or ESC to CANCEL:
```

Figura 16-4 Menú 23.1 Cambio de Contraseña

Paso 4. Introduzca la nueva contraseña en el campo **New Password** (hasta 30 caracteres), y pulse [ENTER].

Paso 5. Teclee nuevamente la nueva contraseña en el campo **Retype to confirm** para confirmación y pulse [ENTER].

Notar que al introducir la contraseña, la pantalla mostrará “*” para cada carácter que se teclee.

Capítulo 17
Configuración General

***Menú 1 – General Setup** contiene información administrativa y relativa al sistema.*

17.1 Configuración General

Menu 1 — General Setup contiene la información administrativa y de sistema (se muestra a continuación). El campo **System Name** tiene la finalidad de identificación. Sin embargo, como algunos ISPs comprueban este nombre, usted debe introducir el nombre de su ordenador.

- En Windows 95/98 click **Inicio, Configuración, Panel de Control, Red.** Click en la pestaña **Identificación**, anotar el dato del campo **Nombre del Equipo** e introducirlo en el campo **System name** del Prestige.
- En Windows 2000 click **Inicio, Configuración, Panel de Control** y hacer doble click en **Sistema.** Click en la pestaña **Identificación de Red** y después en el botón **Propiedades.** Anotar el dato del campo **Nombre del Equipo** e introducirlo en el campo **System name** del Prestige.
- En Windows XP, click **Inicio, Configuración, Panel de Control, Sistema** y click en la pestaña **Nombre del Equipo.** Anotar el dato del campo **Nombre del Equipo** e introducirlo en el campo **System name** del Prestige.

La entrada **Domain Name** es la que se propaga a los clientes DHCP en la Lan. Si se deja en blanco, se usa el nombre de dominio obtenido por DHCP desde el ISP. Mientras usted tiene que introducir el nombre de la máquina (System Name) en cada ordenador, el nombre de dominio puede ser asignado por el Prestige via DHCP.

17.2 Procedimiento para Configurar el Menú 1

Paso 1. Introduzca 1 en el Menú Principal para abrir el Menú 1 – General Setup (mostrado a continuación.

```
Menu 1 - General Setup

System Name= ?
Location=
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No

Route IP= Yes
Bridge= No
 Press ENTER to Confirm or ESC to Cancel:
```

Figura 17-1 Menú 1 General Setup

Paso 2. Complete los campos requeridos. Consulte la tabla siguiente para más información sobre estos campos.

Tabla 17-1 Menú 1 General Setup

CAMPO	DESCRIPCIÓN	EJEMPLO
System Name	Elija un nombre descriptivo para su sistema. El nombre puede incluir hasta 30 caracteres alfanuméricos. No se permiten espacios, pero si los caracteres "-" y "_".	
Location (optional)	Introduzca la localización geográfica (hasta 31 caracteres) de su Prestige.	MyHouse
Contact Person's Name (optional)	Introduzca el nombre (hasta 30 caracteres) de la persona a cargo del Prestige.	JohnDoe
Domain Name	Introduzca el nombre de dominio (si lo conoce). Si deja esta espacio en blanco, el ISP debe asignarte un nombre de dominio via DHCP. Puede ir al menú 24.8 y teclear "sys domainname" para ver el actual nombre de dominio usado por su gateway. Si usted quiere borrar este campo, presione [ESPACIADORA]. El nombre de dominio que usted introduzca tendrá prioridad sobre el que asigne el ISP.	zyxel.com.tw
Edit Dynamic DNS	Pulsar [ESPACIADORA] para seleccionar **Yes** o **No** (defecto). Seleccione **Yes** configurar el **Menu 1.1 — Configure Dynamic DNS** (se discute a continuación).	**No**
Route IP	Seleccione **Yes** para habilitar o **No** para deshabilitar enrutado IP. Deberá habilitar enrutado IP para el acceso a Internet.	**Yes**
Bridge	Active o desactive para protocolos no soportados (ej. SNA) o no active los campos de enrutado anteriores Seleccione **Yes** para activar o **No** para desactivar.	**No**

17.2.1 Procedimiento para Configurar el DNS Dinámico

Si tiene asignada una dirección IP privada en la WAN, no podrá utilizar el DNS Dinámico.

Paso 1. Para configurar el DNS Dinámico, vaya al **Menú 1 – General Setup** y seleccione **Yes** en el campo **Edit Dynamic DNS**. Pulse [ENTER] para mostrar el **Menu 1.1 – Configure Dynamic DNS** como se muestra a continuación.

```
                    Menu 1.1 - Configure Dynamic DNS

       Service Provider = WWW.DynDNS.ORG
       Active= Yes
       Host= me.dyndns.org
       EMAIL= mail@mailserver
       USER= username
       Password= *********
       Enable Wildcard= No

                   Press ENTER to confirm or ESC to cancel:
```

Figura 17-2 Menu 1.1 Configuración DNS Dinámico

Siga las instrucciones de la siguiente tabla para configurar los parámetros del DNS Dinámico.

Tabla 17-2 Menu 1.1 Configuración DNS Dinámico

CAMPO	DESCRIPCIÓN	EJEMPLO
Service Provider	Este es el nombre de su proveedor de servicios DNS Dinámico.	WWW.DynDNS.ORG (defecto)
Active	Pulsar [ESPACIADORA] para seleccionar **Yes** y después pulsar [ENTER] para hacer DNS Dinámico activo.	**Yes**
Host	Introduzca el nombre de dominio asignado a su Prestige por el proveedor DNS Dinámcio.	me.dyndns.org
EMAIL	Introduzca su dirección de correo.	mail@mailserver
USER	Introduzca su nombre de usuario.	
Password	Introduzca el password que se le ha asignado.	
Enable Wildcard	Su Prestige soporta DYNDNS Wildcard. Pulse [ESPACIADORA] y después [ENTER] para seleccionar **Yes** o **No.** Este campo está **N/A** cuando uste elige como cliente DDNS a su proveedor de servicio.	**No**
Cuando haya completado este menú, pulse [ENTER] en el prompt “Press ENTER to Confirm…” para guardar la configuración, o pulse [ESC] en cualquier momento para cancelar.		

Capítulo 18
Configuración Backup de WAN

Este capítulo describe como configurar la redirección de tráfico a través del menú 2.

18.1 Introducción a la Configuración del backup de WAN

Este capítulo explica como configurar el Prestige para las conexiones de la redirección de tráfico.

18.2 Configuración del Dial Backup

En el menú principal, introduzca 2 para abrir el menú 2.

```
                         Menu 2 - Wan Backup Setup

                   Check Mechanism = DSL Link
                   Check WAN IP Address1 = 0.0.0.0
                   Check WAN IP Address2 = 0.0.0.0
                   Check WAN IP Address3 = 0.0.0.0
                     KeepAlive Fail Tolerance = 0
                     Recovery Interval(sec) = 0
                     ICMP Timeout(sec) = 0
                   Traffic Redirect = No

                 Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figura 18-1 Menú 2 Configuración Backup de WAN

La siguiente tabla describe los campos de este menú.

Tabla 18-1 Menú 2 Configuración Backup de WAN

CAMPO	DESCRIPCIÓN
Check Mechanism	Pulse [BARRA ESPACIADORA] y presione [ENTER] para seleccionar el método que utilizará el Prestige para chequear la conexión DSL. Seleccione **DSL Link** para que el Prestige

	compruebe la capa física de la conexión DSL. Seleccione **ICMP** para que el Prestige haga ping periódicamente a determinadas direcciones IP configuradas en los campos **Check WAN IP Address**.
Check WAN IP Address 1-3	Configure estos cmapos para testear la accesibilidad de la WAN de su Prestige. Introduzca la dirección IP de una IP fiable (por ejemplo, la dirección de su servidor DNS). Cuando se está utilizando una conexión de backup, el Prestige hace pings periódicos a estas direcciones configuradas y utiliza la otra conexión de backup (si está configurada) si no hay respuesta.
KeepAlive Fail Tolerante	Introduzca el número de veces (recomendado 2) que el Prestige debe hacer ping a las direcciones IP configuradas en los campos **Check WAN IP Address** sin obtener respuesta antes de saltar a la conexión de backup.
Recovery Interval (seg.)	Cuando el Prestige está utilizando una conexión con prioridad inferior (normalmente una conexión de backup), periódicamente se comprobará si es posible utilizar una conexión de mayor prioridad. Introduzca el número de segundos (se recomiendan 30) que debe esperar el Prestige entre comprobaciones. Permita más tiempo si la dirección IP de destino tiene que soportar mucho tráfico.
ICMP Timeout	Introduzca el número de segundos que una sesión ICMP esperará a la respuesta ICMP.
Traffic Redirect	Pulse la [BARRA ESPACIADORA] para seleccionar **Yes** o **No**. Seleccione **Yes** y pulse [ENTER] para configurar el **Menu 2.1 Traffic Redirect Setup**. Seleccione **No** (por defecto) si no desea configurar esta funcionalidad.
Cuando haya completado este menú, pulse [ENTER] en la línea “Press ENTER to Confirm…” para	

guardar la configuración, o pulse [ESC] en cualquier momento para cancelar.

18.2.1 Configuración de la Redirección del Tráfico

Configure los parámetros que determinan cuando el Prestige enviará el tráfico de la WAN a un gateway de backup utilizando el **Menu 2.1 – Traffic Redirect Setup**.

```
                Menu 2.1 - Traffic Redirect Setup

            Active= No
            Configuration:
              Backup Gateway IP Address= 0.0.0.0
              Metric= 15




            Press ENTER to Confirm or ESC to Cancel:
```

Figura 18-2 Menu 2.1 Configuración de la Redirección de Tráfico

La siguiente tabla describe los campos en este menú.

Tabla 18-2 Menú 2.1 Configuración de la Redirección de Tráfico

CAMPO	DESCRIPCIÓN
Active	Pulse la [BARRA ESPACIADORA] y seleccione **Yes** (para habilitar) y **No** (para deshabilitar) la configuración de la redirección de tráfico. Por defecto está a **No**.
Configuration:	
Backup Gateway IP Address	Introduzca la dirección IP del gateway de bakcup en formato decimal. El Prestige automáticamente enviará el tráfico por esta dirección IP si la conexión a Internet del Prestige se corta.
Metric	Este campo indica la prioridad de esta ruta entre todas las rutas que utiliza el Prestige. La métrica representa el “coste de transmisión”. Un router determina la mejor ruta para la transmisión eligiendo un camino con el menor “coste”. El routing RIP utiliza el contador de saltos como medida del coste, con un mínimo de “1” para conexiones de red directas. El número debe estar entre “1” y “15”, un número mayor de “15” indica que el link está caído. A menor número, menor “coste”.
Cuando haya completado este menú, pulse [ENTER] en la línea “Press ENTER to Confirm…” para	

guardar la configuración, o pulse [ESC] en cualquier momento para cancelar.

Capítulo 19
Configuración LAN

Este capítulo cubre como configurar la red de Área Local cableada (LAN).

19.1 Configuración LAN

Esta sección describe como configurar la Ethernet utilizando el Menu 3 – LAN Setup. Desde el menú principal, introduzca 3 para mostrar el menú 3.

```
                    Menu 3 - LAN Setup

             1. LAN Port Filter Setup
             2. TCP/IP and DHCP Setup


             5. Wireless LAN Setup



                 Enter Menu Selection Number:
```

Figura 19-1 Menú 3 Configuración LAN

19.1.1 Configuración General de la Ethernet

Este menú permite especificar los filtros que se aplicarán al tráfico Ethernet. Raramente se necesitará filtrar el tráfico Ethernet; sin embargo, la configuración de filtros puede ser útil para bloquear ciertos paquetes, reducir el tráfico y prevenir agujeros de seguridad.

```
          Menu 3.1 - LAN Port Filter Setup

      Input Filter Sets:
        protocol filters=
        device filters=
      Output Filter Sets:
        protocol filters=
        device filters=

      Press ENTER to Confirm or ESC to Cancel:
```

Figura 19-2 Menú 3.1 Configuración Filtros del Puerto LAN

Si necesita definir filtros, por favor, consulte en primer lugar el capítulo sobre la Configuración de Filtros, después vuelva a aplicar aquí los filtros.

19.2 Configuración Ethernet Dependiente del Protocolo

Dependiendo de los protocolos de sus aplicaciones, necesitará configurar las respectivas configuraciones Ethernet, como se indica a continuación.

- Para la configuración Ethernet TCP/IP consulte el capítulo referido a la Aplicación del Acceso a Internet.
- Para la configuración Ethernet bridging consulte el capítulo de Configuración Bridging.

19.3 Configuración TCP/IP Ethernet y DHCP

Utilice el menú 3.2 para configurar el TCP/IP de su Prestige.

Para editar el menú 3.2, introduzca 3 en el menú principal para mostrar el **Menu 3 – LAN Setup**. Cuando aparezca el menú 3, pulse 2 y presione [ENTER] para mostrar el Menu **3.2 – TCP/IP and DHCP Ethernet Setup**, como se indica a continuación:

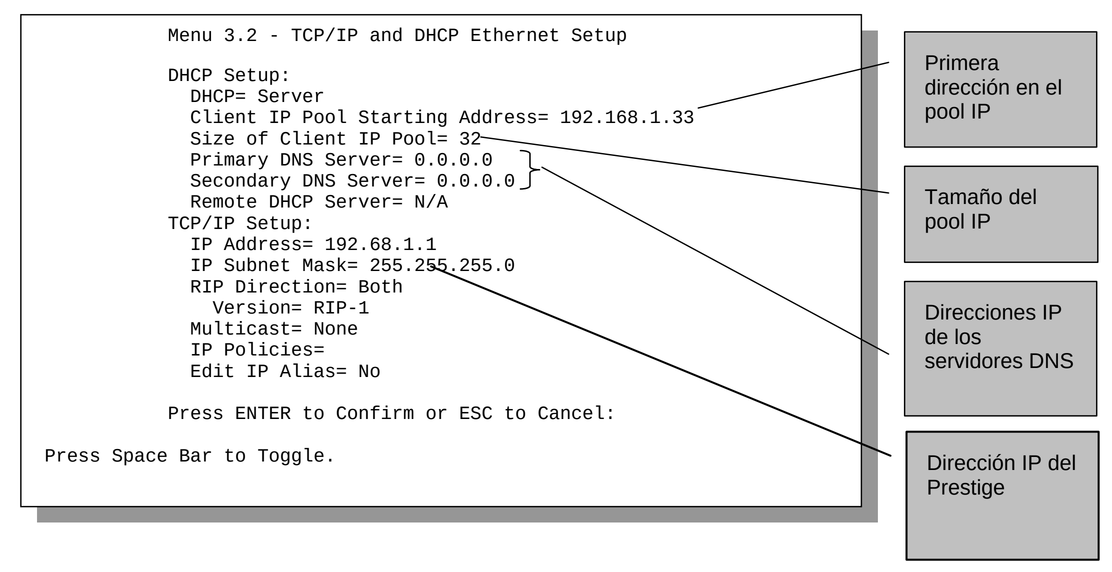


Figura 19-3 Menu 3.2 Configuración Ethernet TCP/IP y DHCP

Siga las intrucciones de la siguiente tabla sobre como configurar los campos del DHCP.

Tabla 19-1 Configuración Ethernet DHCP

CAMPO	DESCRIPCIÓN	EJEMPLO
DHCP Setup		
DHCP	Si tiene el valor **Server**, su Prestige podrá asignar direcciones IP, así como una puerta de enlace por defecto y servidores DNS a Windows 95, Windows NT y otros sistemas que soporten DHCP cliente. Si tiene el valor **None**, el servidor DHCP estará deshabilitado. Si tiene el valor **Relay**, el Prestige actua como sustituto de servidor	**Server** (por defecto)

CAMPO	DESCRIPCIÓN	EJEMPLO
	DHCP, recibiendo y pasando peticiones y respuestas entre el servidor remoto y los clientes. Entre la dirección IP del servidor DCHP remoto si es el caso. Cuando DHCP es usado, los siguientes items son requeridos:	
Client IP Pool Starting Address	Este campo especifica la primera de las contiguas direcciones IP que serán asignadas por el servidor.	192.168.1.33
Size of Client IP Pool	Este campo especifica el tamaño o número de direcciones IP que serán asignadas por el servidor.	32
Primary DNS Server Secondary DNS Server	Entre la dirección IP de los servidores DNS. Los servidores DNS son pasados a los clientes DHCP junto la dirección IP y máscara de subred.	
Remote DHCP Server	Si está seleccionado el valor **Relay** en el campo **DHCP**, entonces introduzca aquí la dirección IP del servidor DHCP remoto.	

Siga las intrucciones que se indican en la siguiente tabla para configurar los parámetros TCP/IP de los puertos Ethernet.

Tabla 19-2 Configuración TCP/IP Ethernet

CAMPO	DESCRIPCIÓN	EJEMPLO
TCP/IP Setup		
IP Address	Introduzca la dirección IP (LAN) de su Prestige en notación decimal.	192.168.1.1
IP Subnet Mask	Su Prestige calculará automáticamente la máscara de subred basandose en la dirección IP que usted asignó. A menos que esté implementando subneting, use la dirección de subred introducida por el Prestige.	255.255.255.0
RIP Direction	Presione [BARRA ESPACIADORA] para seleccionar la dirección RIP. Las opciones són **Both**, **In Only**, **Out Only** o **None**.	**Both** (por defecto)
Version	Presione [BARRA ESPACIADORA] para seleccionar la versión RIP. Las opciones són **RIP-1**, **RIP-2B** o **RIP-2M**.	**RIP-1** (por defecto)
Multicast	IGMP (Internet Group Multicast Protocol) es un protocolo de la capa de sesión usado para establecer miembros en un grupo multicast. El Prestige soporta ambos, IGMP versión 1 (**IGMP-v1**) y versión 2 (**IGMP-v2**). Presione [BARRA ESPACIADORA] para habilitar IP Multicasting o seleccione **None** para deshabilitarlo.	**None** (por defecto)
IP Policies	Cree políticas usando el menú 25 SMT (vea el capítulo *Política de enrutado IP*) y apliquelas en la interfaz LAN del Prestige desde aquí. Puede aplicar hasta cuatro políticas IP (de doce posibles)	2,4,7,9

CAMPO	DESCRIPCIÓN	EJEMPLO
	introduciendo sus números separados por comas.	
Edit IP Alias	El Prestige soporta tres interfaces LAN lógicas via una interfaz Ethernet simple, con el mismo Prestige como puerta de enlace para cada red LAN. Presione [BARRA ESPACIADORA] para cambiar de **No** a **Yes** y presione [ENTER] para ver el menú 3.2.1	**No** (por defecto)

Capítulo 20
Configuración Wireless LAN

Este capítulo cubre como configurar los parámetros Wireless LAN en el menú 3.5.

20.1 Descripción Wireless LAN

Consule este capítulo sobre las pantallas de la wireless LAN para más información sobre la interfaz LAN inalámbrica.

20.2 Configuración Wireless LAN

Utilice el menú 3.5 para configurar su Prestige como un punto de acceso. Para editar el menú 3.5, introduzca 3 en el menú principal para mostrar el **Menu 3 – LAN Setup**. Cuando aparezca el menú 3, pulse 5 y presione [ENTER] para mostrar el **Menu 3.5- Wireless LAN Setup** como se muestra a continuación.

```
          Menu 3.5- Wireless LAN Setup

        ESSID= Wireless
        Hide ESSID = No
        Channel ID= CH01 2412MHz
        RTS Threshold= 2432
        Frag. Threshold= 2432
        WEP= Disable
             Default Key= N/A
             Key1= N/A
             Key2= N/A
             Key3= N/A
             Key4= N/A
        Edit MAC Address Filter= No

        Press ENTER to Confirm or ESC to Cancel:
```

Figura 20-1 Menu 3.5 – Configuración Wireless LAN

La siguiente tabla describe los campos de este menú.

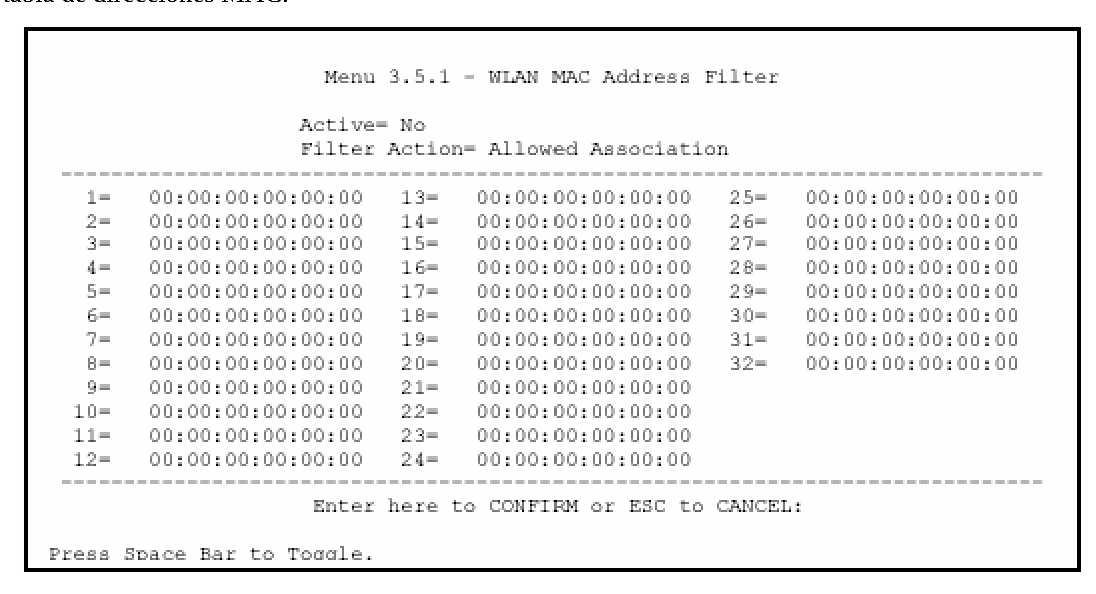
Tabla 20-1 Menú 3.5 – Configuración Wireless LAN

CAMPO	DESCRIPCIÓN	EJEMPLO
ESSID	El ESSID (Extended Service Set IDentifier) identifica el el grupo al que el cliente wireless está asociado. Los clientes wireless asociados a un punto de acceso tienen que tener el mismo ESSID. Introduzca un nombre descriptivo (hasta 32 caracteres) para el Identificador wireless.	**Wireless**
Hide ESSID	Pulsar [ESPACIADORA] y seleccionar **Yes** para ocultar ESSID en la trama inicial de salida para que ninguna estación externa pueda obtener el ESSID a través de un escaneo pasivo.	**No**
Channel ID	Pulsar [ESPACIADORA] para seleccionar un canal. Esto le permite configurar la frecuencia de operación/canal dependiendo de su región. Las posibles elecciones son **CH01 2412MHz**, **CH02 2417MHz**, **CH03 2422MHzCH11 2462MHz CH04 2427MHz**, **CH05 2432MHz**, **CH06 2437MHz**, **CH07 2442MHz**, **CH08 2447MHz**, **CH09 2452MHz**, **CH10 2457MHz** or **CH11 2462MHz**.	**CH01 2412MHz**
RTS Threshold	El umbral RTS(Request To Send) (número de bytes) habilita la comunicación RTS/CTS). Los datos con el tamaño de trama mayor que este valor implementarán la comunicación RTS/CTS. Configurando este atributo para que sea mayor que el tamaño máximo del MSDU (Unidad de Datos de Servicio MAC) se elimanará la opción de que se produzca la comunicación RTS/CTS. Introducir un valor entre 0 y 2432.	**2432**
Frag. Threshold	El umbral(número de bytes) para la fragmentación de mensajes dirigidos. El el tamaño máximo de datos fragmentados que se pueden enviar. Introducir un valor entre 256 y 2432	**2432**
WEP Encryption	WEP (Wired Equivalent Privacy) proporciona encriptación de datos para evitar que estaciones puedan ver lo que se está transmitiendo por la red wireless. Selccionando **Disable** permite a todos los clientes comunicarse con el punto de acceso sin encriptación de datos. Seleccione **64-bit WEP** o **128-bit WEP** para el tipo de encriptación.	**Disable**
Default Key	Introduzca el número de la clave que va estar activa.	
Key 1 to Key 4	Si elige **64-bit WEP** en el campo **WEP Encryption**, introduzca 5 caracteres o 10 dígitos hexadecimales (“0-9”,”A-F”) precedido por 0x para cada clave (1-4). Si elige **128-bit WEP** en el campo **WEP Encryption,** entonces introduzca 13 caracteres o 26 dígitos hexadecimales (“0-9”,”A-F”) precedido por 0x para cada clave (1-4). Hay 4 claves de encriptación para asegurar sus datos de escuchas externas de usuarios wireless no autorizados. Los valores para las claves deben estar configuradas de igual forma tanto en el punto de acceso como en los clientes wireless.	

CAMPO	DESCRIPCIÓN	EJEMPLO
Edit MAC Address Filter	Para editar la tabla de filtrado de direcciones MAC, pulse [ESPACIADORA] y seleccione **Yes** y pulse [ENTER] para abrir el menú 3.5.1.	**No**
Cuando haya completado este menú, pulse [ENTER] en el prompt “Press ENTER to confirm or ESC to cancel” para guardar su configuración o presione [ESC] para cancelar y volver a la página anterior.		

20.2.1 Filtrado MAC en la LAN Inalámbrica

El siguiente nivel de seguridad es el filtrado de direcciones MAC. Para permitir a una estación wireless asociarse con el Prestige, introduzca la dirección MAC de la tarjeta wireless LAN en la estación wireless en la tabla de direcciones MAC.



```
                    Menu 3.5.1 - WLAN MAC Address Filter

                  Active= No
                  Filter Action= Allowed Association
------------------------------------------------------------------------------
  1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
  2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
  3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
  4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
  5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
  6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
  7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
  8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
  9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
 10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
 11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
 12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
------------------------------------------------------------------------------
                   Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figura 20-2 Menu 3.5.1 Filtrado de Direcciones MAC

La siguiente tabla describe los campos de este menú.

Tabla 20-2 Menú 3.5.1 Filtrado de Direcciones MAC

CAMPO	DESCRIPCIÓN
Active	Para habilitar el filtrado por direcciones MAC, pulsar [ESPACIADORA] y seleccionar **Yes** y pulsar [ENTER].
Filter Action	Definir la acción del filtro para la lista de direcciones MAC que están en la tabla de filtrado de direcciones MAC. Para denegar el acceso al Prestige, pulsar [ESPACIADORA] y seleccionar **Deny Association** y pulsar [ENTER]. Las direcciones MAC que no se encuentren en la lista podrán acceder al router. La acción por defecto, **Allowed Association**, permite asociarse con el Prestige. A las direcciones MAC que no estén en la lista se les denegará el acceso al router.
MAC Address Filter	
Address 1..	Introduzca las direcciones MAC (en formato XX:XX:XX:XX:XX:XX) de los ordenadores de los clientes a los que se le permite o deniega el acceso al Prestige en estos campos de direcciones.
Cuando haya completado este menú, pulse {ENTER] en el prompt “Press ENTER to confirm or ESC to cancel” para guardar su configuración o pulse [ESC] para cancelar y volver al menú anterior.	

Capítulo 21
Acceso a Internet

Este capítulo muestra como configurar la LAN y WAN del Prestige para el Acceso a Internet.

21.1 Descripción del Acceso a Internet

Consulte los capítulos sobre el asistente del configurador web, las pantallas LAN y WAN para más información sobre los campos de las pantallas del SMT cubiertas en este capítulo.

21.2 Políticas IP

Tradicionalmente, el enrutamiento está basado exclusivamente en la dirección de destino y el router toma el camino más corto para enviar el paquete. Las políticas de enrutamiento IP (IPPR) proporcionan un mecanismo para superponerse sobre el comportamiento del enrutamiento por defecto y alteran la política de envio de los paquetes basándose en políticas definidas por el administrador de red. El enrutamiento basado en políticas se aplica a los paquetes entrantes por interfaz, con prioridad sobre el enrutamiento común. Se pueden crear políticas utilizando el menú 25 (ver el capítulo de Políticas de Enrutamiento IP) y aplicarlas en los interfaces LAN y/o WAN utilizando los menús 3.2 (LAN) y 11.3 (WAN).

21.3 IP Alias

El IP Alias permite la partición de una red física en diferentes redes lógicas utilizando el mismo interfaz Ethernet. El Prestige soporta 3 interfaces LAN lógicas a través de su única interfaz LAN física con el mismo Prestige como puerta de enlace para cada red de LAN.

Asegúrese que las subredes lógicas de la LAN no se solapan entre sí.

La siguiente figura muestra una LAN dividida en subredes A, B y C.

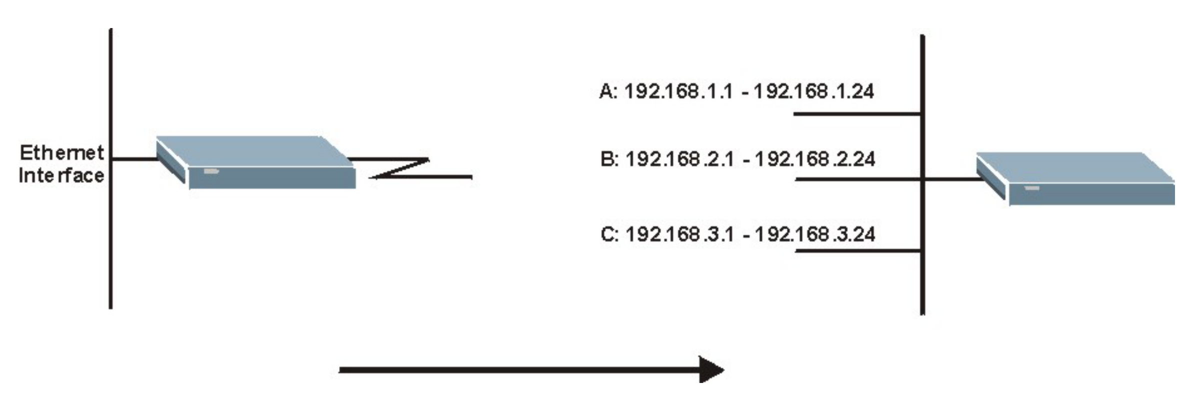


Figura 21-1 Red Física

Figura 21-2 Partición de Redes Lógicas

Utilice el menú 3.2.1 para configurar el IP Alias en su Prestige.

21.4 Configuración IP Alias

Utilice el menú 3.2 para configurar la primera red. Mueve el curso hasta el campo **Edit IP Alias** y pulse sobre la [BARRA ESPACIADORA] para seleccionar **Yes** y presione [INTRO] para configurar la segunda y tercera red.

```
                    Menu 3.2 - TCP/IP and DHCP Setup

                    DHCP Setup:
                     DHCP= Server
                     Client IP Pool Starting Addres= 192.168.1.33
                     Size of Client IP Pool= 32
                     Primary DNS Server= 0.0.0.0
                     Secondary DNS Server= 0.0.0.0
                     Remote DHCP Server= N/A
                    TCP/IP Setup:
                      IP Address= 192.168.1.1
                      IP Subnet Mask= 255.255.255.0
                      RIP Direction= None
                        Version= N/A
                      Multicast= None
                      IP Policies=
                      Edit IP Alias= Yes

                    Press ENTER  to confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figura 21-3 Menú 3.2 Configuración TCP/IP y DHCP

Pulse [INTRO] para mostrar el **Menu 3.2.1 – IP Alias Setup**, como aparece a continuación.

```
                    Menu 3.2.1 - IP Alias Setup

                IP Alias 1= No
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  RIP Direction= N/A
                  Version= N/A
                  Incoming protocol filters= N/A
                  Outgoing protocol filters= N/A
                IP Alias 2= No
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  RIP Direction= N/A
                  Version= N/A
                  Incoming protocol filters= N/A
                  Outgoing protocol filters= N/A

                 Enter here to CONFIRM or ESC to CANCEL:
```

Figura 21-4 Menú 3.2.1 Configuración IP Alias

Siga las instrucciones de la siguiente tabla para configurar los parámetros del IP Alias.

Tabla 21-1 Menú 3.2.1 Configuración IP Alias

CAMPO	DESCRIPCIÓN	EJEMPLO
IP Alias	Seleccione **Yes** para configurar la red LAN del Prestige.	Yes
IP Address	Introduzca la dirección IP de su Prestige en formato decimal	192.168.1.1
IP Subset Mask	El Prestige automáticamente calculará la máscara de subred basándose en la dirección IP introducida. A menos que esté utilizando subredes, utilice la máscara de subred que ha calculado el Prestige.	255.255.255.0
RIP Direction	Pulse la [BARRA ESPACIADORA] para seleccionar la dirección del RIP. Seleccione **None, Both, In Only** u **Out Only**.	None
Version	Pulse la [BARRA ESPACIADORA] para seleccionar la versión de RIP. Escoja entre **RIP-1, RIP-2B** o **RIP-2M**.	RIP-1
Incoming Protocol Filtres	Introduzca los filtros que desea aplicar a los paquetes entrantes a través de este interfaz.	
Outgoing Protocol Filtres	Introduzca los filtros que desea aplicar a los paquetes salientes a través de este interfaz.	

Cuando haya completado este menú, pulse [INTRO] en la línea del mensaje “Press ENTER to Confirm…” para guardar la configuración, o pulse [ESC] en cualquier momento para cancelar.

21.5 Configuración Enrutamiento IP

El primer paso es habilitar el enrutamiento IP en el Menú 1 – General Setup.

Para editar el menú 1, introduzca 1 en el menú principal y pulse [INTRO]. Configure el campo **Route IP** a **Yes** pulsando la [BARRA ESPACIADORA].

```
                Menu 1 - General Setup

             System Name= ?
             Location= location
             Contact Person's Name=
             Domain Name=
             Edit Dynamic DNS= No

             Route IP= Yes
             Bridge= No

            Press ENTER to Confirm or ESC to Cancel:
```

Figura 21-5 Menú 1 Configuración General

21.6 Configuración del Acceso a Internet

El menú 4 permite la introducción de los parámetros para el acceso a internet. El menú 4 es en la actualidad un menú simplificado de uno de los nodos remotos accesible a través del menú 11. Antes de configurar el Prestige para el acceso a Internet, necesitará tener toda la información relativa a su cuenta de acceso al servicio.

Utilice la tabla de Información de la Cuenta de Internet en la Guía Rápida para guardar dicha información. Si la encapsulación que utiliza es PPPoA o PPPoE, entonces la única información de su ISP que necesitará será un nombre de usuario y una contraseña. Sólo necesitará conocer la dirección IP de la puerta de enlace en el caso de estar utilizando una encapsulación ENET ENCAP.

Desde el menú principal, introduzca 4 para mostrar el Menu 4 – Internet Access Setup, como aparece a continuación.

```
Menu 4 - Internet Access Setup

ISP's Name= MyIsp
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 8
VCI #= 32
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Dynamic
  IP Address= N/A
Network Address Translation= SUA Only
  Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Figura 21-6 Menú 4 Configuración Acceso a Internet

La siguiente tabla contiene instrucciones sobre como configurar el Prestige para el acceso a Internet.

Tabla 21-2 Menú 4 Configuración Acceso a Internet

CAMPO	**DESCRIPCIÓN**	**EJEMPLO**
ISP's Name	Introduzca el nombre de su Proveedor de Servicio de Internet. Esta información es meramente informativa.	MyISP
Encapsulación	Pulse [BARRA ESPACIADORA] para seleccionar el método de encapsulación utilizado por su ISP. Escoja entre **PPPoE, PPPoA, RFC1483** o **ENET ENCAP**.	ENET ENCAP
Multiplexing	Pulse [BARRA ESPACIADORA] para seleccionar el método de multiplexado utilizado por su ISP. Escoja entre **VC-based** o **LLC-based**.	LLC-based
VPI #	Introduzca el Identificador de Camino Virtual (VPI)	8
VCI #	Introduzca el Identificador de Canal Virtual (VCI)	32
ATM QoS Type	Pulse [BARRA ESPACIADORA] y seleccione **CBR** (Continuos Bit Rate – Tasa de Bit Continua) para especificar un ancho (siempre) fijo. Seleccione **UBR** (Unspecified Bit Rate – Tasa de Bit sin Especificar) para aplicaciones que no son sensibles al retardo, tales como el e-mail. Seleccione **VBR** (Variable Bit Rate – Tasa de Bit Variable) para tráfico en ráfagas y compartición del ancho de banda con otras aplicaciones.	UBR

Peak Cell Rate (PCR)	Ésta es la máxima tasa a la que el transmisor puede enviar celdas. Introduzca el PCR.	0
Sustain Cell Rate (SCR)	Éste campo indica la tasa media de celdas de una ráfaga. Introduzca el SCR; debe ser menor que el PCR.	0
Maximum Burst Size (MBS)	Se refiere al máximo número de celdas que pueden ser transmitidas a la tasa PCR. Introduzca el MBS. El valor deberá ser menor que 65535.	0
My Login	Configure los campos **My Login** y **My Password** únicamente para encapsulaciones **PPPoA** y **PPPoE**. Introduzca el nombre de usuario que su ISP le proporcione.	N/A
My Password	Introduzca la contraseña asociada con el nombre de usuario anterior.	N/A
ENET ENCAP Gateway	Introduzca la dirección IP del gateway proporcionado por su ISP cuando utilice encapsulación ENET ENCAP.	N/A
Idle Timeout	Este valor especifica el número de segundos de inactividad que transcurren antes de que el Prestige automáticamente desconecte la sesión PPPoE.	0
IP Address Assignment	Pulse la [BARRA ESPACIADORA] para seleccionar asignación **Estática (Static)** o **Dinámica (Dynamic).**	Dynamic
IP Address	Introduzca la dirección IP suministrada por su ISP se aplica.	N/A
Network Address Translation	Pulse la [BARRA ESPACIADORA] para seleccionar **None, SUA Only** o **Full Feature**. Por favor, consulte el Capítulo NAT para más detalles sobre la funcionalidad SUA.	SUA Only
Address Mapping Set	Introduzca el número de reglas de mapeo (1-8) para utilizarlo con NAT. Vea el capítulo NAT para más detalles.	N/A
Cuando haya completado este menú, pulse [INTRO] en la línea del mensaje “Press ENTER to confirm…” para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla previa.		

Si toda la configuración es correcta su Prestige debería conectarse automáticamente a Internet. Si la conexión falla, anote el mensaje de error que reciba en pantalla y lleve a cabo los pasos indicados en la resolución de problemas.

Capítulo 22
Configuración de Nodos Remotos

Este capítulo cubre la parte relativa a la configuración de nodos remotos.

22.1 Descripción de la Configuración de Nodos Remotos

Esta sección describe los parámetros de configuración de los nodos remotos. Un nodo remoto es necesario para lanzar llamadas a un gateway remoto. Un nodo remoto representa tanto el gateway remoto como la red tras el a través de la conexión WAN. Cuando se utiliza el menú 4 para configurar el acceso a Internet, se está configurando uno de los nodos remotos.

En primer lugar es necesario seleccionar un nodo remoto en el Menú 11 – Remote Node Setup. Entonces podrá editar el perfil del nodo en el menú 11.1, así como configurar parámetros específicos en tres submenús ; editar las opciones bridge e IP en el menú 11.e; editar las opciones ATM en el menú 11.6; y editar la configuración de filtros en el menú 11.5.

22.2 Configuración de un Nodo Remoto

Esta sección decribe los parámetros independientes del protocolo para cada nodo remoto.

22.2.1 Perfil de Nodo Remoto

Para configurar un nodo remoto, siga los siguientes pasos:

Paso 1. Desde el menú principal, introduzca 11 para mostrar el Menu 11 – Remote Node Setup.

Paso 2. Cuando aparezca el menú 11, como se indica a continuación, introduzca el número del nodo remoto que desee configurar.

```
                Menu 11 - Remote Node Setup

            1. My ISP (ISP, SUA)
            2. ________
            3. ________
            4. ________
            5. ________
            6. ________
            7. ________
            8. ________


                  Enter Node # to Edit:
```

Figura 22-1 Menú 11 Configuración Nodo Remoto

22.2.2 Encapsulación y Multiplexación

Para el acceso a Internet deberá usar los métodos de encapsulación y multiplexación utilizados por su ISP. El método o métodos a utilizar dependerá también de cuántos VCs tenga y cuántos protocolos de red diferentes necesite. Aquí se muestran algunos ejemplos de las combinaciones más adecuadas en cada aplicación.

Escenario 1. Un VC, Múltiples protocolos

Encapsulación **PPPoA** (RFC-2364) con multiplexación **VC-based** es la mejor combinación porque no se necesitan cabeceras extra de identificación del protocolo. El protocolo **PPP** ya contiene esta información.

Escenario 2. Un VC, Un Protocolo (IP)

Seleccione la encapsulación **RFC-1483** con multiplexación **VC-based** que requiere la menor carga de cabecera (0 octetos). Sin embargo, si existe una necesidad potencial de suportar múltiples protocolos en un futuro, sería recomendable seleccionar la encapsulación **PPPoA** en lugar de **RFC-1483**, de manera que no necesite un posterior reconfiguración.

Escenario 3. Múltiples VCs

Si dispone de un número igual (o mayor) de VCs que de protocolos, entonces seleccione encapsulación **RFC-1483** y multiplexación **VC-based**.

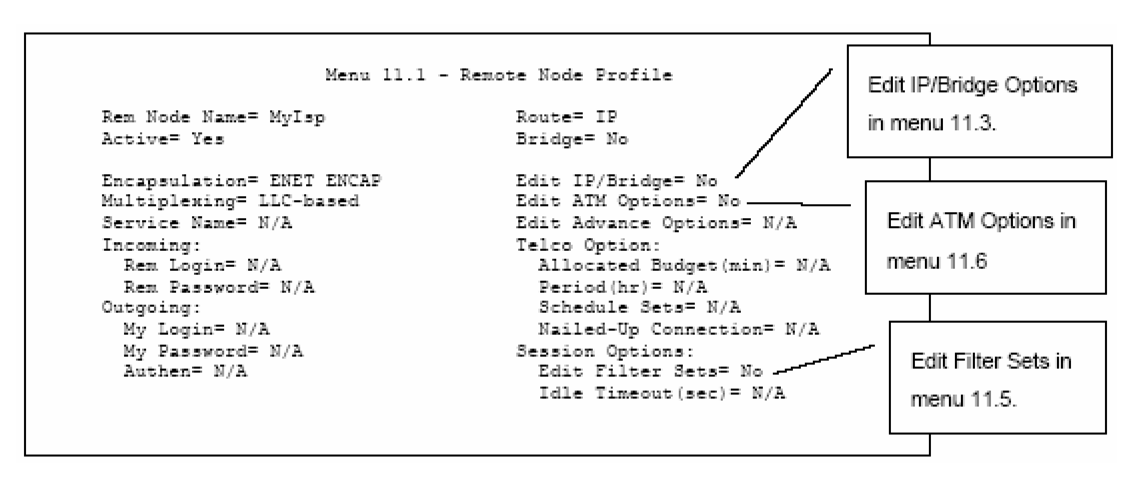


Figura 22-2 Menú 11.1 Perfil Nodo Remoto

En el **Menú 11.1 – Perfil Nodo Remoto**, complete los campos como se describe en la siguiente tabla.

Tabla 22-1 Menú 11.1 Perfil Nodo Remoto

CAMPO	DESCRIPCIÓN	EJEMPLO
Rem Node Name	Introduzca un nombre único y descriptivo de hasta ocho caracteres para este nodo.	MyISP
Active	Pulse la [BARRA ESPACIADORA] y presione [INTRO] para seleccionar **Yes** y activar o **No** para desactivar este nodo. Los nodos inactivos se muestran con un signo "-" en el menú 11.	Yes
Encapsulation	**PPPoA** hace referencia al RFC-2364 (Encapsulación PPP sobre AAL5) Si se selecciona **RFC-1483** o **ENET ENCAP**, entonces los campos **Rem Login, Rem Password, My Login, My Password** y **Authen** pasan a estar no aplicables (N/A).	ENET ENCAP
Multiplexing	Presione [BARRA ESPACIADORA] y pulse [INTRO] para seleccionar el método de multiplexación que utiliza su ISP, bien **VC-based** o **LLC-based**.	LLC-based
Service Name	Cuando utilice la encapsulación **PPPoE**, introduzca el nombre de servicio PPPoE.	N/A
Incoming:		

Rem Login	Introduzca el nombre de usuario que utilizará este nodo remoto para llamar al Prestige. Este nombre de usuario y el Rem Password serán utilizados para autenticar a este nodo.	
Rem Password	Introduzca la contraseña utilizada cuando este nodo remoto llame al Prestige.	
Outgoing:		
My Login	Introduzca el nombre de usuario asignado por su ISP cuando el Prestige llama al nodo remoto.	
My Password	Introduzca la contraseña asignada por su ISP cuando el Prestige llama a este nodo remoto.	
Authen	Este campo indica el protocolo de autenticación utilizado para las llamadas salientes. La opciones para este campo son: **CHAP/PAP** – Su Prestige aceptará tanto CHAP como PAP cuando le sea requerido por el nodo remoto. **CHAP –** Acepta sólo **CHAP** (Challenge Handshake Authentication Protocol). **PAP** – Acepta únicamente **PAP** (Password Authentication Protocol).	
Route	Este campo determina el protocolo utilizado para el enrutamiento. Las opciones son **IP** o **None**.	IP
Bridge	Cuando es bridging está habilitado, el Prestige reenviará cualquier paquete que no enrute hacia este nodo remoto; en cualquier otro caso, los paquetes serán descartados. Seleccione **Yes** para habilitar y **No** para deshabilitar.	No
Edit IP/Bridge	Presione [BARRA ESPACIADORA] para seleccionar **Yes** y pulse [INTRO] para mostrar el **Menu 11.3 – Remote Node Network Layer Options.**	No
Edit ATM Options	Presione [BARRA ESPACIADORA] para seleccionar **Yes** y pulse [INTRO] para mostrar el **Menu 11.6 – Remote Node ATM Layer Options.**	No
Edit Advance Options	Este campo sólo estará disponible cuando se seleccione **PPPoE** en el campo Encapsulation. Presione [BARRA ESPACIADORA] para seleccionar **Yes** y pulse [INTRO] para mostrar el **Menu 11.8 – Advance Setup Options**.	No

Telco Option		
Allocated Budget (min)	Este campo configura un máximo para el tiempo de una llamada saliente hacia este nodo remoto. Por defecto este campo está a 0 lo que significa que no hay control de tiempo	
Period (hr.)	Este campo es el perido de tiempo en el que el control de tiempo será reseteado. Por ejemplo, si se nos permite llamar a este nodo remoto un máximo de 10 minutos cada hora, entonces el campo **Allocated Budget** es (10 minutos) y el campo **Period** es 1 (hora).	
Schedule Sets	Este campo sólo es aplicable para encapsulación **PPPoE** y **PPPoA**. Para más detalles consulte el capítulo de Configuración de Control de Llamadas.	
Nailed up Connection	Este campo sólo es aplicable para encapsulación **PPPoE** y **PPPoA**. Este campo especifica si se desea tener una conexión siempre establecida con este nodo remoto. Se pueden encontrar más detalles dentro de este capítulo.	
Session Options		
Edit Filter Sets	Utilice [BARRA ESPACIADORA] para seleccionar **Yes** y pulse [INTRO] para abrir el menú 11.5 y editar las reglas de filtrado. Vea la sección del Filtrado de Nodo Remoto para más detalle.	No (defecto)
Idle Timeout (seg.)	Introduzca el número de segundos (0-9999) que pueden pasar cuando el Prestige está inactivo (no existe tráfico hacia este nodo remoto), antes de que el Prestige automáticamente desconecte el nodo remoto. 0 indica que la sesión nunca será desconectada por inactividad.	
Cuando haya completado este menú, pulse [INTRO] sobre la línea de mensaje "Press ENTER to confirm…." Para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla previa.		

22.2.3 Protocolo de Autenticación de Salida

Por razones obvias, debería emplear el protocolo de autenticación más potente posible. Sin embargo, la implementación de algunos fabricantes incluye protocolos de autenticación específicos en el perfil de usuario. Se producirá la desconexión si el protocolo negociado es diferente del definido en el perfil de usuario, incluso aunque el protocolo negociado es más potente que el especificado. Si el par remoto desconecta justo tras la autenticación, asegúrese que ha especificado un protocolo de autenticación correcto.

22.3 Opciones de Capa de Red para Nodo Remoto

Para los parámetros TCP/IP, lleve a cabo los siguientes pasos para editar el **Menú 11.3 – Remote Node Network Layer Options** como se muestra.

Paso 1. En el menú 11.1, asegúrese que **IP** está entre los protocolos del campo **Route**.

Paso 2. Mueva el cursor hasta el campo **Edit IP/Bridge**, presione [BARRA ESPACIADORA] para seleccionar **Yes,** entonces pulse [INTRO] para mostrar el **Menu 11.3 – Remote Node Network Layer Options**.

```
                Menu 11.3 - Remote Node Network Layer Options

     IP Options:                          Bridge Options:
        IP Address Assignment= Dynamic      Ethernet Addr Timeout (min)= N/A
        Rem IP Addr: 0.0.0.0
        Rem Subnet Mask= 0.0.0.0
        My WAN Addr= N/A
        NAT= Full Feature
          Address Mapping Set= 2
        Metric= 2
        Private= No
        RIP Direction= None
           Version= RIP-1
        Multicast= None
        IP Policies= 3,4,5,6

  Press ENTER to Confirm or ESC to Cancel:
```

Figura 22-3 Menú 11.3 – Opciones de Capa de Red del Nodo Remoto

La siguiente tabla explica los campos del Menú 11.3.

Tabla 22-2 Menú 11.3 – Opciones de Capa de Red del Nodo Remoto

CAMPO	DESCRIPCIÓN	EJEMPLO
IP Address Assignment	Presione [BARRA ESPACIADORA] y después [INTRO] para seleccionar **Dynamic** si el nodo remoto utiliza una asignación de dirección IP dinámica o **Static** si se utiliza una dirección IP fija. Sólo será posible configurar esto en el nodo del ISP, el resto de nodos están configurados con Static.	Dynamic
Rem IP Addr	Ésta es la dirección IP introducida en el menú anterior	
Rem Subnet Mask	Introduzca la máscara de subred asignada por el nodo remoto.	
My WAN Addr	Algunas implementaciones, especialmente derivadas de UNIX, requieren unos números de red IP separados para los enlaces de WAN y LAN y cada extremo a tener una dirección única dentro del número de red de la WAN. En este caso, introduzca la dirección IP asignada al puerto WAN del	

	Prestige. NOTA : Referido a la dirección local del Prestige, no a la dirección del router remoto.	
NAT	Presione [BARRA ESPACIADORA] y pulse [INTRO] para seleccionar **Full Feature** si tiene múltiples direcciones IP públicas para su Prestige. Seleccione **SUA Only** si dispone de una sólo dirección IP pública en la WAN de su Prestige. El SMT utiliza el conjunto 255 del Mapeo de Direcciones (menu 15.1 –ver la sección 29.3.1). Seleccione **None** para deshabilitar el NAT.	SUA Only
Address Mapping Set	Cuando se selecciona **Full Feature** en el campo NAT, configure los conjuntos de mapeo de direcciones en el menú 15.1. Seleccione uno de los conjuntos de servidores NAT (2-10) en el menú 15.2 (consulte el capítulo NAT para más detalles) e introduzca aquí el número.	2
Metric	La métrica representa el "coste" de la transmisión para propósitos de enrutamiento. El enrutamiento IP utiliza el contador de saltos como medida del coste, con un mínimo de 1 para redes conectadas directamente. Introduzca un número que aproxime el coste para este enlace. El número no tiene que ser preciso, pero debe estar entre 1 y 15. En la práctica, 2 o 3 es normalmente un buen número.	2
Private	Este campo determina si el Prestige incluirá la ruta a este nodo remoto en los broadcasts RIP. Si está puesto a **Yes**, esta ruta se mantiene privada y no se incluye en los broadcasts de RIP. Si está a **No**, este ruta al nodo remoto será propagada a otros hosts a través de los broadcasts de RIP.	No
RIP Direction	Presione [BARRA ESPACIADORA] y después [INTRO] para seleccionar la dirección RIP. Las opciones son **Both, In Only, Out Only** o **None**.	None
Version	Presione [BARRA ESPACIADORA] y después [INTRO] para seleccionar la versión RIP. Las opciones son **RIP-1, RIP-2B** o **RIP-2M**.	RIP-1
Multicast	**IGMP-v1** habilita el IGMP versión 1, **IGMP-v2** habilita el IGMP versión 2 y **None** deshabilita el IGMP.	None
IP Policies	Es posible aplicar hasta 4 conjuntos de políticas IP (de 12) introduciendo sus números separados por comas. Configure estos conjuntos previamente en el menú 15 (vea el capítulo de Políticas de Enrutamiento IP) y posteriormente aplíquelas aquí.	3,4,5,6
Cuando haya completado este menú, pulse [INTRO] en la línea con el mensaje "Press ENTER to confirm…" para guardar la configuración o [ESC] para cancelar y volver a la pantalla previa.		

22.3.1 Muestras de Direcciones IP en Mi Dirección WAN

La siguiente figura utiliza muestras de direcciones IP para ayudar a comprender este campo de Mi Dirección WAN (My WAN Addr) en el menú 11.3. Consulte la figura previa de Direcciones LAN y WAN en el capítulo del configurador web en la configuración LAN para una breve revisión de lo que es la IP de WAN. **My WAN Addr** indica la IP WAN local del Prestige (172.16.0.1 en la siguiente figura) mientras que **Rem IP Addr** indica la dirección IP WAN del par (172.16.0.2 en la siguiente figura).

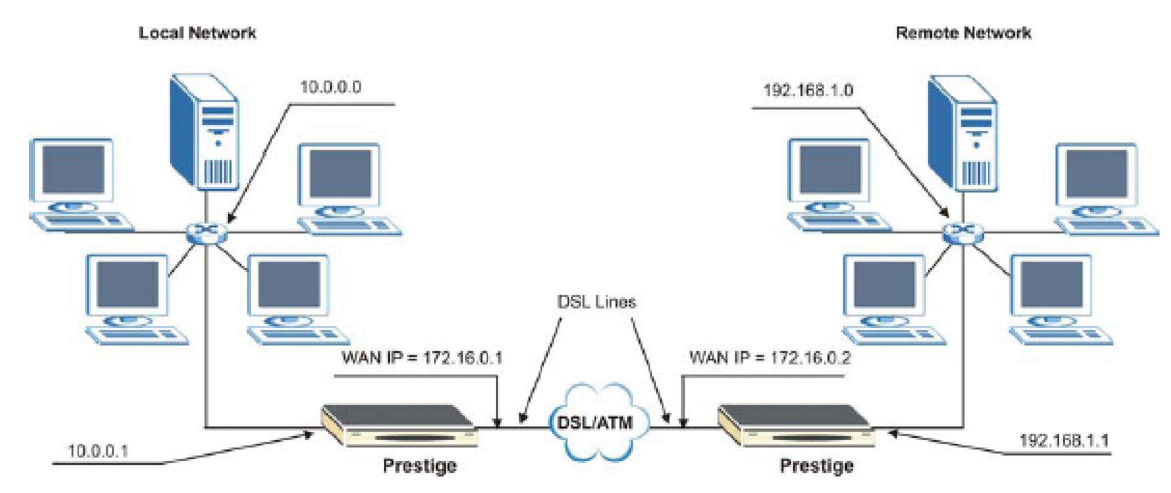


Figura 22-4 Muestra de direcciones IP para una conexión TCP/IP LAN-to-LAN

22.4 Filtrado en Nodo Remoto

Mueva el cursor al campo **Edit Filter Set** en el menú 11.1, a continuación presione [BARRA ESPACIADORA] para seleccionar **Yes**. Pulse [INTRO] para mostrar el **Menú 11.5 – Remote Node Filter**.

Utilice el Menú 11.5 – Remote Node Filter para especificar los filtros aplicar al tráfico entrante y saliente entre este nodo remoto y el Prestige; así como para prevenir que ciertos paquetes puedan lanzar llamadas. Podrá especificar hasta 4 conjuntos de filtros separados por comas, por ejemplo, 1,5,9,12, en cada campo.

Hacer notar que los espacios son aceptados en este campo. El Prestige tiene unos filtros preconfigurados, NetBIOS_WAN, que bloquean los paquetes NetBIOS. Incluya éste en los filtros de llamadas si se desea prevenir que los paquetes NetBIOS lancen llamadas a nodos remotos.

```
Menu 11.5 - Remote Node Filter

     Input Filter Sets:
       protocol filters= 11, 12
         device filters=
     Output Filter Sets:
       protocol filters=
         device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

Figura 22-5 Menu 11.5 Remote Node Filter (Encapsulación RFC 1483 o ENET)

```
Menu 11.5 - Remote Node Filter

     Input Filter Sets:
       protocol filters= 11, 12
         device filters=
     Output Filter Sets:
       protocol filters=
         device filters=
       Call Filter Sets:
       Protocol filters=
         Device filters=

Enter here to CONFIRM or ESC to CANCEL:
```

Figura 22-6 Menu 11.5 Remote Node Filter (Encapsulación PPPoA o PPPoE)

22.5 Opciones de Edicción de Capa ATM

Siga los siguientes pasos mostrados a continuación para editar el **Menu 11.6 – Remote Node ATM Layer Options.**

En el menú 11.1, mueva el cursor hasta el campo **Edit ATM Options** y después presione [BARRA ESPACIADORA] para seleccionar **Yes**. Pulse [INTRO] para mostrar el **Menu 11.6 – Remote Node ATM Layer Options**.

Existen dos versiones del menú 11.6 para el Prestige, dependiendo de la multiplexación **VC-based/LLC-based** y encapsulación **PPP** que se seleccione en el menú 11.1.

22.5.1 Multiplexación VC-based (sin encapsulación PPP)

Para multiplexación VC-based, por acuerdo previo, un protocolo es asignado a un circuito virtual específico, por ejemplo, VC1 transportará IP. Números de VPI y VCI separados deberán especificarse para cada protocolo.

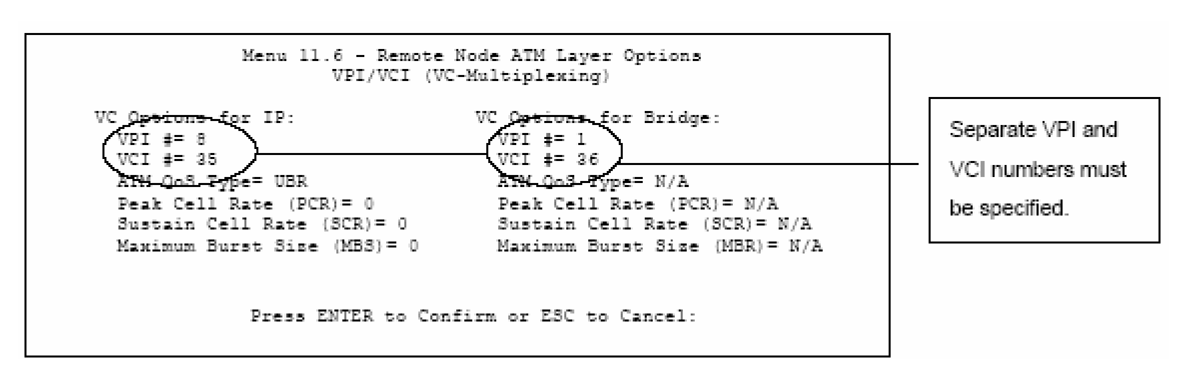


Figura 22-7 Menú 11.6 para Multiplexación VC-based

22.5.2 Multiplexación LLC-based o Encapsulación PPPoE

Para multiplexación LLC-based y encapsulación PPP, un VC transporta múltiples protocolos con información de identificación de protocolo contenida en la cabecera de cada paquete.

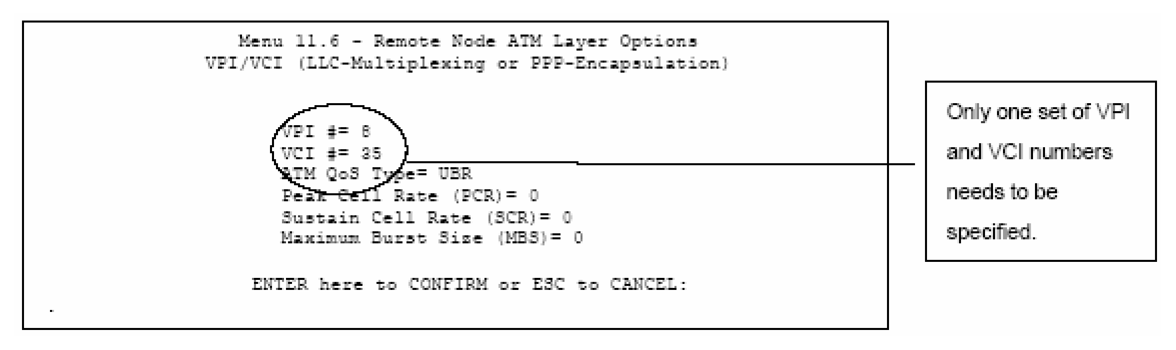


Figura 22-8 Menu 11.6 para Multiplexación LLC-based o Encapsulación PPP

En este caso, únicamente será necesario especificar un conjunto de VPI y VCI para todos los protocolos. El rango válido para el VPI será entre 0 y 255 y para el VCI entre 32 y 65535 (del 1 al 31 está reservados para gestión local del tráfico ATM).

22.5.3 Opciones de Configuración Avanzadas

En el menú 11.1, seleccione **PPPoE** en el campo **Encapsulation**.

```
                    Menu 11.1 - Remote Node Profile

  Rem Node Name= MyISP                    Route= IP
  Active= Yes                             Bridge= No

  Encapsulation= PPPoE                    Edit IP/Bridge= No
  Multiplexing= LLC-based                 Edit ATM Options= No
  Service Name=                           Edit Advance Options= Yes
  Incoming:                               Telco Option:
    Rem Login=                              Allocated Budget(min)= 0
    Rem Password= ********                  Period(hr)= 0
  Outgoing:                                 Schedule Sets=
    My Login= ?                             Nailed-Up Connection= No
    My Password= ?                        Session Options:
    Authen= CHAP/PAP                        Edit Filter Sets= No
                                            Idle Timeout(sec)= 0

                 Press ENTER to Confirm or ESC to Cancel:
```

Figura 22-9 Menu 11.1 Perfil de Nodo Remoto

Mueva el cursor hasta el campo **Edit Advance Options**, presione [BARRA ESPACIADORA] para seleccionar **Yes,** y después pulse [INTRO] para mostrar el **Menu 11.8 – Advance Setup Options**.

```
                Menu 11.8 - Advance Setup Options

         PPPoE pass-through= No



         Press ENTER to Confirm or ESC to Cancel:
```

Figura 22-10 Menu 11.8 Opciones de Configuración Avanzadas

La siguiente tabla describe los campos de este menú.

Tabla 22-3 Menu 11.8 Opciones de Configuración Avanzadas

CAMPO	DESCRIPCIÓN
PPPoE pass-through	Presione [BARRA ESPACIADORA] para seleccionar **Yes** y pulse [INTRO] para habilitar el PPPoE pass-through. Adicionalmente al cliente PPPoE integrado en el Prestige, es posible habilitar que el PPPoE pase a través del Prestige desde hasta 10 hosts en la LAN utilizando software de cliente PPPoE en sus ordenadores para conectarse con su ISP a través del Prestige. Cada host puede tener una cuenta separada y una dirección pública WAN. El PPPoE pass-through es una alternativa al NAT para aplicaciones donde el NAT no es apropiado.

	Presione [BARRA ESPACIADORA] para seleccionar No y pulse [INTRO] para deshabilitar el PPPoE pass-through si no necesita permitir a ningún host de la LAN el utilizar software de cliente PPPoE en sus ordenadores para conectarse con el ISP.
Cuando haya completado este menú, presione [INTRO] sobre la línea de mensaje “Press ENTER to confirm….” Para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla previa.	

Capítulo 23
Configuración Rutas Estáticas

Este capítulo muestra como configurar rutas estáticas.

23.1 Descripción Rutas Estáticas IP

Las rutas estáticas indican al Prestige información de enrutamiento que no puede ser aprendida automáticamente a través de otros medios. Esto puede darse en casos en los que el RIP está deshabilitado en la LAN o cuando una red remota está más allá del nodo remoto al que se está directamente conectado.

Cada nodo remoto especifica sólo la red a la que el gateway está directamente conectado y el Prestige no tiene conocimiento de las redes que hay más allá. Por ejemplo, el Prestige tiene conocimiento de la red N2 de la siguiente figura a través del nodo remoto del Router 1. Sin embargo, el Prestige es incapaz de enlutar un paquete a la red N3 porque no conoce la existencia de una ruta a través del nodo remoto del Router 1 (a través del Router 2). Las rutas estáticas permiten darle a conocer al Prestige acerca de estas redes situadas más allá de los nodos remotos.

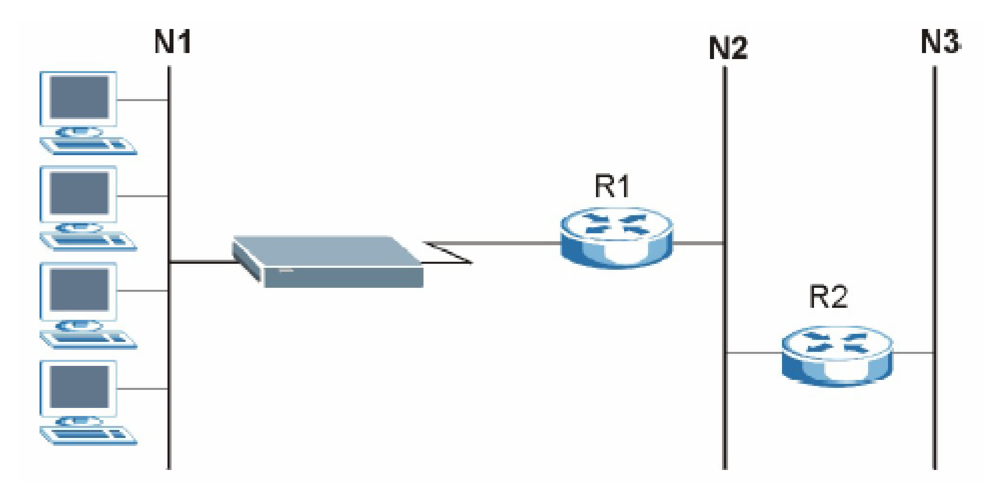


Figura 23-1 Ejemplo de Topología de Enrutamiento Estático

23.2 Configuración

Paso 1. Para configurar una ruta estática, utilice el menú 12 – Static Route Setup (mostrado a continuación).

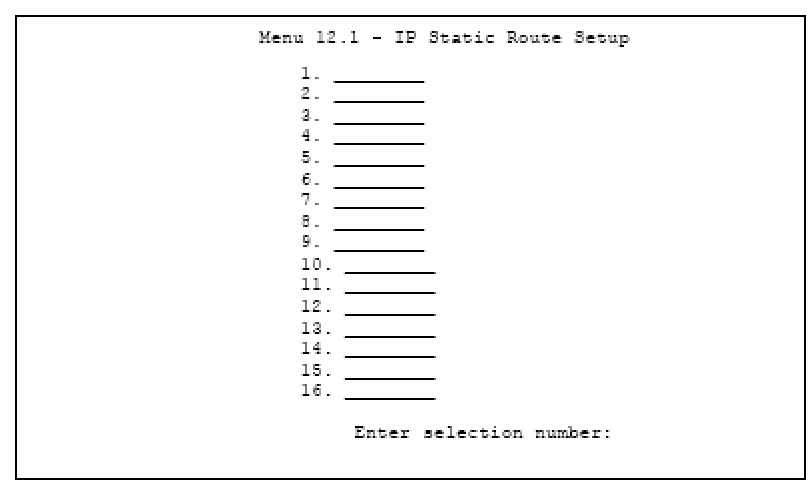
```
Menu 12 - Static Route Setup

        1. IP Static Route
        3. Bridge Static Route


 Please enter selection:
```

Figura 23-2 Menú 12 Configuración Rutas Estáticas

Paso 2. Desde el menú 12, seleccione 1 para abrir el Menu 12.1 – IP Static Route Setup (mostrado a continuación).



```
Menu 12.1 - IP Static Route Setup

    1. ________
    2. ________
    3. ________
    4. ________
    5. ________
    6. ________
    7. ________
    8. ________
    9. ________
    10. ________
    11. ________
    12. ________
    13. ________
    14. ________
    15. ________
    16. ________

        Enter selection number:
```

Figura 23-3 Menu 12.1 Configuración Rutas Estáticas IP

Paso 3. Ahora, introduzca el número de la ruta que desea configurar.

```
Menu 12.1.1 - Edit IP Static Route

    Route #: 1
    Route Name= ?
    Active= No
    Destination IP Address= ?
    IP Subnet Mask= ?
    Gateway IP Address= ?
    Metric= 2
    Private= No

Press ENTER to Confirm or ESC to Cancel:
```

Figura 23-4 Menú 12.1.1 Edición Rutas Estáticas IP

La siguiente tabla describa los campos del **Menu 12.1.1 – Edición de Rutas Estáticas IP**

Tabla 23-1 Menu 12.1.1 Edición Rutas Estáticas IP

CAMPO	DESCRIPCIÓN
Route #	Éste es el número de índice de la ruta estática seleccionada en el menú 12.1
Route Name	Introduzca un nombre descriptivo para esta ruta. Con fines meramente informativos.
Destination IP Address	Este parámetro especifica la dirección de red IP del destino final. El enrutamiento se basa siempre en un número de red. Si necesita especificar una ruta a un único host, utilice como máscara de subred 255.255.255.255 en el campo de máscara de subred para forzar que el número de red sea idéntico al identificador del host.
IP Subnet Mask	Introduzca la máscara de subred para este destino. Siga la discusión sobre Máscara de Subred IP en este manual.
Gateway IP Address	Introduzca la dirección IP del gateway. El gateway es el nodo continuo al Prestige que enviará el paquete a su destino. En la LAN, el gateway debe ser un router en el mismo segmento de red que el Prestige; sobre la WAN, el gateway debe ser la dirección IP de uno de los nodos remotos.
Metric	La métrica representa el “coste” de la transmisión. El enrutamiento IP utiliza el salto como medida del coste, con un mínimo de 1 para redes conectadas directamente. Introduzca un número que aproxime el coste para este enlace. El número no tiene que ser preciso, pero debe encontrarse entre 1 y 15. En la práctica, 2 ó 3 es un buen número.
Private	Este parámetro determina si el Prestige incluirá esta ruta al nodo remoto en su broadcast RIP. Si se configura a Yes, esta ruta se mantiene privada y no será incluida en el broadcast RIP. Si está a No, la ruta al nodo remoto será propagada a otros hosts a través del broadcast RIP.
Cuando haya completado este menú, presione [INTRO] en la línea de mensaje “Press ENTER to confirm….” para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla previa.	

Capítulo 24
Configuración Bridging

Este capítulo muestra como configurar los parámetros de bridging en su Prestige.

24.1 Bridging en General

El bridging basa su decisión de envío en el MAC (Media Access Control), o dirección hardware, mientras que el routing se basa en la dirección de red (IP). El bridging permite al Prestige transportar paquetes de protocolos de capa de red que no enruta, por ejemplo, SNA, desde una red a otra. La advertencia es que, comparado con el routing, el bridging genera más tráfico para el mismo protocolo de capa de red, y además requirere más ciclos de CPU y memoria.

Por razones de eficiencia, no habilite el bridging a menos que necesite soportar protocolos diferentes a IP en su red. Para IP, habilite el routing si lo necesita; no haga bridge de lo que el Prestige puede enlutar.

24.2 Configuración Ethernet Bridge

Básicamente, todos los paquetes no locales son puenteados hacia la WAN. El Prestige no soporta IPX.

24.2.1 Configuración Nodo Remoto Bridging

Siga el procedimiento de una sección anterior para configurar los parámetros independientes del protocolo en el **Menu 11.1 – Remote Node Profile**. Para parámetros relativos al bridging, necesitará configurar el **Menu 11.3 – Remote Node Network Layer Options**.

Para configurar el Menu 11.3 – Opciones de Capa de Red del Nodo Remoto mostrado en la siguiente figura, siga los siguientes pasos:

Paso 1. En el menú 11.1, asegúrese que el campo **Bridge** está en **Yes**.

```
                     Menu 11.1 - Remote Node Profile

     Rem Node Name= ?                       Route= IP
     Active= Yes                            Bridge= Yes

     Encapsulation= ENET ENCAP              Edit IP/Bridge= No
     Multiplexing= VC-based                 Edit ATM Options= No
     Service Name= N/A                      Edit Advance Options= N/A
     Incoming:                              Telco Option:
       Rem Login= N/A                         Allocated Budget(min)= N/A
       Rem Password= N/A                      Period(hr)= N/A
     Outgoing:                                Schedule Sets= N/A
       My Login= N/A                          Nailed-Up Connection= N/A
       My Password= N/A                     Session Options:
       Authen= N/A                            Edit Filter Sets= No
                                              Idle Timeout(sec)= N/A

                 Press ENTER to Confirm or ESC to Cancel:
```

Figura 24-1 Menu 11.1 Perfil de Nodo Remoto

Paso 2. Mueva el cursor hasta el campo **Edit IP/Bridge**, entonces presione [BARRA ESPACIADORA] para colocar el valor a **Yes** y pulse [INTRO] para editar el **Menu 11.3 – Remote Node Network Layer Options**.

```
                Menu 11.3 - Remote Node Network Layer Options

     IP Options:                         Bridge Options:
      IP Address Assignment= Static       Ethernet Addr Timeout (min)= 0
      Rem IP Addr: 0.0.0.0
        Rem Subnet Mask= 0.0.0.0
        My WAN Addr= 0.0.0.0
        NAT= Full Feature
          Address Mapping Set=2
        Metric= 2
        Private= No
        RIP Direction= Both
          Version= RIP-2B
        Multicast= IGMP-v2
        IP Policies=

   Press ENTER to Confirm or ESC to Cancel:
```

Figura 24-2 Menu 11.3 Opciones de Capa de Red del Nodo Remoto

Tabla 24-1 Opciones de Capa de Red del Nodo Remoto : Campos Bridge

CAMPO	DESCRIPCIÓN
Bridge (menú 11.1)	Asegúrese que este campo está a Yes.
Edit IP/Bridge (menú 11.1)	Pulse [BARRA ESPACIADORA] para seleccionar Yes y presione [INTRO] para mostrar el menú 11.3.

Ethernet Addr Timeout (min.) (menú 11.3)	Introduzca el tiempo (en minutes) que el Prestige retendrá información de Direcciones Ethernet en sus tablas internas mientras la línea está caída. Si esta información es retenida, el Prestige no tendrá que recompilar las tablas cuando la línea vuelva a estar levantada.
Cuando haya completado este menú, presione [INTRO] en la línea de mensaje "Press ENTER to confirm…" para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla previa.	

24.2.2 Configuración de Rutas Estáticas Bridge

De forma similar a las rutas estáticas de nivel de red, un ruta estática de bridging informa al Prestige sobre cuál es la ruta a un nodo antes de que una conexión esté establecida. Las rutas estáticas bridge se configuran en el menú 12.3.1 (ir al menú 12, escoja la opción 3, a continuación elija la ruta estática a editar) como se muestra a continuación.

```
                    Menu 12.3.1 - Edit Bridge Static Route

                    Route #: 1
                    Route Name=
                    Active= No
                    Ether Address= ?
                    IP Address=
                    Gateway Node= 1



                   Press ENTER to Confirm or ESC to Cancel:
```

Figura 24-3 Menu 12.3.1 Edición de Rutas Estáticas Bridge

La siguiente tabla describe el menú de **Edición de Rutas Estáticas Bridge**.

Tabla 24-2 Menú 12.3.1 Edición de Rutas Estáticas Bridge

CAMPO	DESCRIPCIÓN
Route #	Éste es el índice de la ruta que introdujo en el Menu 12.3 – Bridge Static Route Setup.
Route Name	Introduzca un nombre para la ruta estática bridge para propósitos de identificación.
Active	Indica si la ruta estática está activa (Yes) o no (No).
Ether Address	Introduzca la dirección MAC del ordenador de destino al que se quiere hacer bridge de los paquetes.
IP Address	Si está disponible, introduzca la dirección IP del ordenador de destino al que se desea hacer bridge de los paquetes.

Gateway Node	Pulse [BARRA ESPACIADORA] y después [INTRO] para seleccionar el número del nodo remoto (1 a 8) que será el gateway para esta ruta.
Cuando haya completado este menú, pulse [INTRO] en la línea de mensaje “Press ENTER to confirm….” Para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla previa.	

Capítulo 25
Network Address Translation (NAT)

Este capítulo discute sobre como configurar el NAT en el Prestige.

25.1 Utilizando NAT

25.1.1 SUA (Single User Account) frente a NAT

SUA (Single User Account – Cuenta Única de Usuario) es una implementación de ZyNOS como subconjunto del NAT que soporta 2 tipos de mapeo, **Many-to-One** y **Server.** Vea la sección 29.3.1 para una descripción más detallada sobre la configuración del NAT para SUA. El Prestige también soporta **Full Feature** NAT para mapear múltiples direcciones IP globales a múltiples direcciones IP privadas de LAN.

1.- Seleccione **SUA Only** si sólo tiene una dirección IP pública en la WAN para su Prestige.

2.- Seleccione **Full Feature** si dispone de múltiples direcciones IP públicas para su Prestige.

25.2 Aplicando el NAT

El NAT se aplica a través del menú 4 o 11.3 como se indica a continuación. La siguiente figura muestra como se aplica el NAT para el acceso a Internet en el menú 4. Introduzca 4 desde el menú principal para ir al **Menu 4 – Internet Access Setup.**

```
Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-1 Menu 4 Aplicando NAT para el Acceso a Internet

La siguiente figura muestra como aplicar NAT al nodo remoto en el menú 11.1.

Paso 1. Introduzca 11 desde el menú principal.

Paso 2. Cuando aparezca el menú 11, como se indica en la siguiente figura, introduzca el número del nodo remoto que desea configurar.

Paso 3. Mueva el cursor al campo **Edit IP/Bridge**, presione [BARRA ESPACIADORA] para seleccionar **Yes** y a continuación pulse [INTRO] para mostrar el **Menu 11.3 – Remote Node Network Layer Options**.

```
                    Menu 11.3 - Remote Node Network Layer Options

  IP Options:                                 Bridge Options:
    IP Address Assignment = Dynamic             Ethernet Addr Timeout(min)= N/A
    Rem IP Addr = 0.0.0.0
    Rem Subnet Mask= 0.0.0.0
    My WAN Addr= N/A
    NAT= SUA Only
      Address Mapping Set= N/A
    Metric= 2
    Private= No
    RIP Direction= None
      Version= RIP-1
    Multicast= None
    IP Policies=


                    Enter here to CONFIRM or ESC to CANCEL:
```

Figura 25-2 Menu 11.3 Aplicando NAT al Nodo Remoto

La siguiente tabla describe las opciones de la Traslación de Direcciones de Red (NAT).

Tabla 25-1 Aplicando NAT en los menus 4 y 11.3

CAMPO	DESCRIPCIÓN	EJEMPLO
NAT	Presione [BARRA ESPACIADORA] y a continuación [INTRO] para seleccionar **Full Feature** si dispone de múltiples direcciones IP públicas en la WAN del Prestige. El SMT utiliza un mapeo de direcciones que se configuran y se introduce en el campo **Address Mapping Set** (menu 15.1 – ver sección 29.3.1)	**Full Feature**
	Seleccione **None** para deshabilitar el NAT	**None**
	Cuando se seleccione **SUA Only**, el SMT utiliza el conjunto de mapeos 255 (menu 15.1 – ver sección 29.3.1). Escoja **SUA Only** si sólo tiene una dirección IP pública en la WAN de su Prestige.	**SUA Only**

25.3 Configuración NAT

Utilice los menús y submenús del mapeo de direcciones para crear tablas de mapeo utilizadas para asignar direcciones globales a ordenadores de la LAN. El **conjunto 255** es utilizado para el SUA. Cuando se selecciona **Full Feature** en el menú 4 ó 11.3, el SMT utilizará el conjunto 1. Cuando se seleccione **SUA Only**, el SMT utilizará el **conjunto 255** preconfigurado (sólo lectura).

El conjunto servidor (Server) es una lista de servidor en la LAN a puertos externos. Para usar este conjunto, una regla servidor debe ser configurada dentro del mapeo de direcciones NAT. Por favor, consulte la sección sobre redirección de puertos en el capítulo del configurador NAT a través del web para más información sobre estos menús. Para configurar NAT, introduzca 15 en la pantalla principal para mostrar la siguiente pantalla.

```
                Menu 15 - NAT Setup

               1. Address Mapping Sets
               2. NAT Server Sets


                    Enter Menu Selection Number:
```

Figura 25-3 Menú 15 Configuración NAT

25.3.1 Mapeo de Direcciones

Introduzca 1 para mostrar el **Menu 15.1 – Address Mapping Sets**.

```
                         Menu 15.1 - Address Mapping Sets

                         1.
                         2.
                         3.
                         4.
                         5.
                         6.
                         7.
                         8.
                       255. SUA (read only)


                           Enter Menu Selection Number:

Enter Menu Selection Number:
```

Figura 25-4 Menú 15.1 Mapeo de Direcciones

Mapeo de Direcciones SUA

Introduzca 255 para mostrar la siguiente pantalla (ver también la sección 25.1.1). Los campos en este menú no pueden ser modificados.

```
                    Menu 15.1.255 - Address Mapping Rules

 Set Name=

Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
 2.                                    0.0.0.0                           Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                 Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-5 Menú 15.1.255 Mapeo de Direcciones SUA

La siguiente tabla explica los campos en este menú.

El menú 15.1.255 es de sólo lectura.

Tabla 25-2 Mapeo de Direcciones SUA

CAMPO	DESCRIPCIÓN	EJEMPLO
Set Name	Éste es el nombre del conjunto seleccionado en el menú 15.1 o introduzca un nuevo nombre si se desea crear un nuevo conjunto de reglas.	SUA
Idx	Éste es el índice o número de regla.	1
Local Start IP	**Local Start IP** es la dirección IP local de inicio (ILA).	0.0.0.0
Local End IP	**Local End IP** es la dirección IP final (ILA). Si la regla se aplica para todas las IPs locales, entonces la Local Start IP será 0.0.0.0 y la Local End IP será 255.255.255.255	255.255.255.255
Global Start IP	Ésta es la dirección IP global de inicio (IGA). Si tiene una dirección IP dinámica, introduzca 0.0.0.0 como **Global Start IP**.	0.0.0.0
Global End IP	Ésta es la dirección IP global final.	
Type	Éstos son los tipos de mapeos. El **Server** permite especificar múltiples servidores de diferentes tipos tras el NAT. Vea capítulos posteriores con algunos ejemplos.	Server

Cuando haya completado este menú, presiones [INTRO] en la línea de mensaje "Press ENTER to confirm…" para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla previa.

Mapeo de Direcciones definidas por el Usuario

Ahora vamos a ver la opción 1 del menú 15.1. Introduzca 1 para Mostrar este menú. Sólo veremos las diferencias con el menú previo. Indicar que la presencia de los campos Action y Select Rule muestran la posibilidad de configurar reglas en esta pantalla. También hacer ver que el símbolo [?] en el campo Set Name indica que es un campo obligatorio y es necesario introducir un nombre para este conjunto.

```
                        Menu 15.1.1 - Address Mapping Rules

  Set Name= NAT_SET

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1.
  2
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.

                  Action= Edit          Select Rule=

                  Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-6 Menú 15.1.1 Primer Conjunto

Si el campo ***Set Name*** se deja en blanco, el conjunto entero será eliminado.

Los campos Type, Local y Global Start/End IPs se configuran en el menú 15.1.1.1 (descrito a continuación) y los valores se muestran aquí.

Ordenación de Reglas

El ordenar las reglas es importante porque el Prestige aplica las reglas en el orden que se especifican. Cuando una regla coincide con el paquete, el Prestige lleva a cabo la respectiva acción y las reglas restantes son ignoradas. Si hay más de una regla vacía antes de una regla configurada, la regla configurada será colocada delante de las reglas vacías. Por ejemplo, si ya ha configurado de la regla 1 a la 6 y ahora

configura la regla número 9. En el resumen de este conjunto, la nueva regla aparecerá en el índice 7 y no en el 9.

Ahora si se borra la regla 4, de la regla 5 a la 7 serán subidas hacia arriba una posición, de manera que la antigua regla 5 será la nueva regla 4, la antigua regla 6 será la nueva regla 5 y la antigua 7 será la nueva 6.

Tabla 25-3 Menú 15.1.1 Primer Conjunto de Reglas de Mapeo

CAMPO	DESCRIPCIÓN	EJEMPLO
Set Name	Introduzca el nombre para este conjunto de reglas. Éste es un campo obligatorio. Si este campo se deja en blanco, el conjunto completo será eliminado.	NAT_SET
Action	Por defecto está en **Edit**. **Edit** significa que se quiere editar la regla seleccionada (ver el siguiente campo). **Insert Before** significa insertar una nueva regla antes de la regla seleccionada. Las reglas tras la regla seleccionada serán movidas hacia abajo una regla. **Delete** quiere decir el eliminar la regla seleccionada y a continuación subir las siguientes reglas una posición. **None** deshabilita la opción de **Seleccionar Regla (Select Rule)**.	Edit
Select Rule	Cuando se selecciona **Edit, Insert Before** o **Delete** en el campo anterior, el cursor salta a este campo para permitir seleccionar la regla para aplicar la acción en cuestión.	1

Pulse **[INTRO]** al final de la pantalla para guardar el conjunto completo. Será necesario hacer esto nuevamente si se realiza algún cambio en el conjunto – incluyendo el borrado de una regla. No se guardará ningún cambio hasta que se lleve a cabo esta acción.

Seleccionando **Edit** en el campo **Action** y seleccionando una regla, se nos mostrará el siguiente menú, **Menu 15.1.1.1 – Address Mapping Rule** en el que se podrá editar una regla individual y configurar los campos **Type, Local** y **Global Start/End IPs**.

La dirección en un campo End IP siempre tendrá que ser numéricamente mayor que su correspondiente dirección Start IP.

```
                    Menu 15.1.1.1 Address Mapping Rule

          Type= One-to-One

          Local IP:
            Start=
            End  = N/A

          Global IP:
            Start=
            End  = N/A

          Server Mapping Set= N/A

                Press ENTER to Confirm or ESC to Cancel:

      Press Space Bar to Toggle.
```

Figura 25-7 Menu 15.1.1.1 Edición/Configuración de una regla individual en un Conjunto

La siguiente tabla explica los campos de este menú.

Tabla 25-4 Menu 15.1.1.1 Edición/Configuración de una regla individual en un Conjunto

CAMPO	DESCRIPCIÓN	EJEMPLO
Type	Presione [BARRA ESPACIADORA] y a continuación [INTRO] para seleccionar de un total de cinco tipos. Existen los mapeos definidos en el capítulo correspondiente al NAT en las pantallas del configurador web. **Server** permite especificar múltiples servidores de diferentes tipos tras el NAT. Vea un ejemplo en la sección 25.5.3.	One-to-One
Local IP	Los campos local IP son **N/A** para el tipo Server; los campos Global IP deben estar configurados para tipo **Server**.	
Start	Ésta es la dirección IP local de inicio (ILA).	0.0.0.0
End	Ésta es la dirección IP local final (ILA). Si la regla se va a aplicar a todas las IPs locales, entonces el campo Start IP será 0.0.0.0 y el	N/A

	campo End IP será 255.255.255.255. Este campo será **N/A** para los tipos One-to-One y Server.	
Global IP		
Start	Éste es la dirección global inicial (IGA). Si tiene una dirección dinámica, introduzca 0.0.0.0 en el campo **Global IP Start**. Indicar que el campo **Global IP Start** podrá ser 0.0.0.0 para los tipos **Many-to-One** o **Server**.	0.0.0.0
End	Ésta es la dirección global final (IGA). Este campo será **N/A** para los tipos **One-to-One, Many-to-One** y **Server**.	N/A
Sever Mapping Set	Sólo disponible cuando el tipo configurado es Server. Introduzca un número de 1 a 10 para escoger el conjunto de servidores definidos en el menú 15.2.	
Cuando haya completado este menú, presione [INTRO] en la línea de mensaje "Press ENTER to confirm…" para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla previa.		

25.4 Configuración de un Servidor tras el NAT

Siga los siguientes pasos para configurar un servidor tras el NAT:

Paso 1. Introduzca 15 en el menú principal para ir al **Menu 15 – NAT Setup**.

Paso 2. Introduzca 2 para mostrar el **Menu 15.2 –NAT Server Sets** como se indica a continuación.

```
                 Menu 15.2 - NAT Server Sets

              1. Server Set 1 (Used for SUA Only)
              2. Server Set 2
              3. Server Set 3
              4. Server Set 4
              5. Server Set 5
              6. Server Set 6
              7. Server Set 7
              8. Server Set 8
              9. Server Set 9
             10. Server Set 10


                Enter Set Number to Edit:
```

Figura 25-8 Menu 15.2 Conjunto Servidores NAT

Paso 3. Introduzca 1 para ir al **Menu 15.2.1 – NAT Server Setup** como se indica.

```
                    Menu 15.2 - NAT Server Setup

        Rule   Start Port No.   End Port No.   IP Address
       ---------------------------------------------------
         1.      Default          Default        0.0.0.0
         2.        21               21           192.168.1.33
         3.        0                0            0.0.0.0
         4.        0                0            0.0.0.0
         5.        0                0            0.0.0.0
         6.        0                0            0.0.0.0
         7.        0                0            0.0.0.0
         8.        0                0            0.0.0.0
         9.        0                0            0.0.0.0
        10.        0                0            0.0.0.0
        11.        0                0            0.0.0.0
        12.        0                0            0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-9 Menu 15.2.1 – Configuración Servidores NAT

Paso 4. Introduzca un número de puerto que no esté en uso en el campo **Start Port No**. Para abrir sólo un puerto, introduzca el mismo número de puerto en el campo **End Port No**. Para especificar un rango de puertos, introduzca el último puerto del rango a ser abierto en el campo **End Port No**.

Paso 5. Introduzca la dirección IP interna del servidor en el campo IP Address. En la siguiente figura, aparece un ordenador actuando como servidor FTP, Telnet y SMTP (puertos 21, 23 y 25) con dirección 192.168.1.33.

Paso 6. Pulse [INTRO] en la línea con el mensaje “Press ENTER to confirm…” para guardar la configuración tras haber definido todos los servidores o pulse [ESC] en cualquier momento para cancelar.

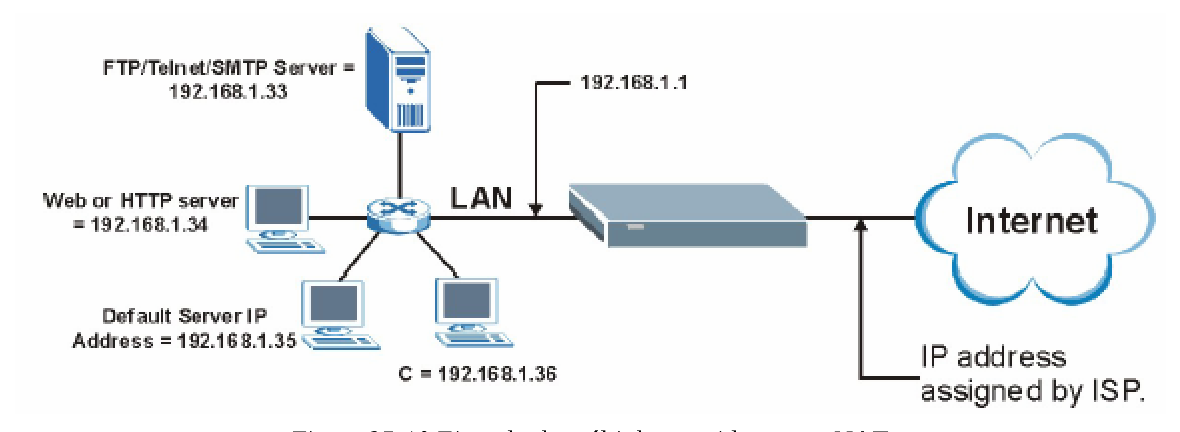


Figura 25-10 Ejemplo de múltiples servidores tras NAT

25.5 Ejemplos NAT General

A continuación se muestran algunos ejemplos de configuración NAT.

25.5.1 Ejemplo 1 : Sólo Acceso a Internet

En el siguiente ejemplo de acceso a Internet, únicamente es necesario configurar una regla dónde todas las direcciones locales se mapearán a la dirección global dinámica asignada por su ISP.

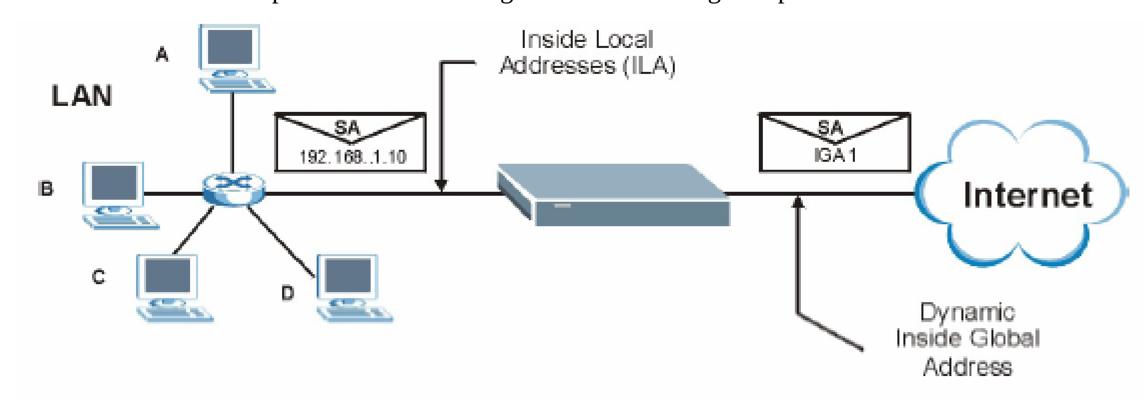


Figura 25-11 Ejemplo 1

```
        Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-12 Menu 4 – Acceso a Internet y Ejemplo NAT

Desde el menú 4, seleccionar la opción **SUA Only** en el campo **Network Address Translation**. Éste es el mapeo Many-to-One discutido en la sección 29.5. La opción de sólo lectura **SUA Only** en el campo **Network Address Translation** en los menús 4 y 11.3 se encuentra preconfigurado especialmente para soportar este caso.

25.5.2 Ejemplo 2 : Acceso a Internet con un Servidor Interno

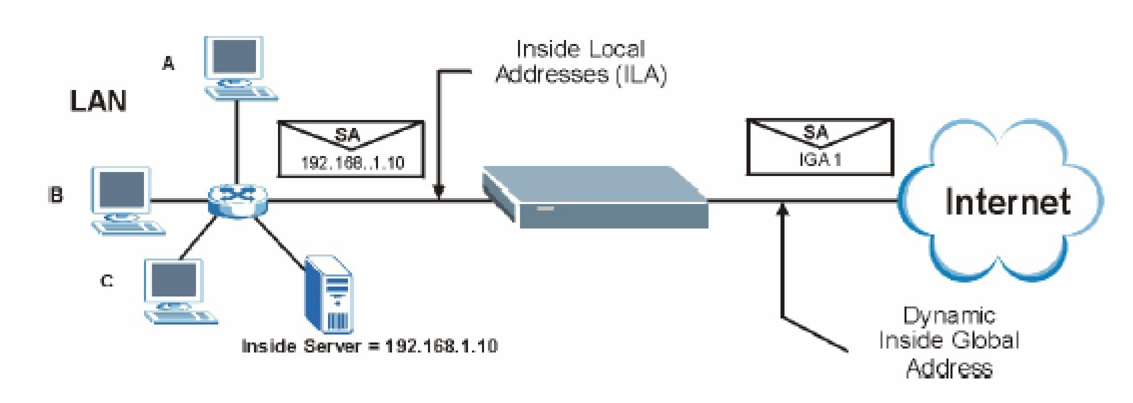


Figura 25-13 Ejemplo 2

En este caso, es necesario llevar a cabo el mismo procedimiento que se ha indicado en el ejemplo anterior (utilizar la configuración **SUA Only**) y adicionalmente ir al menú 15.2 para especificar el Servidor Interno tras el NAT como se indica en la siguiente figura.

```
           Menu 15.2.1 - NAT Server Setup (Used for SUA Only)

          Rule   Start Port No.   End Port No.   IP Address
         ---------------------------------------------------
            1.     Default           Default          192.168.1.10
            2.      0                 0            0.0.0.0
            3.      0                 0            0.0.0.0
            4.      0                 0            0.0.0.0
            5.      0                 0            0.0.0.0
            6.      0                 0            0.0.0.0
            7.      0                 0            0.0.0.0
            8.      0                 0            0.0.0.0
            9.      0                 0            0.0.0.0
           10.      0                 0            0.0.0.0
           11.      0                 0            0.0.0.0
           12.      0                 0            0.0.0.0

                Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-14 Menu 15.2 Especificación de un Servidor Interno

25.5.3 Ejemplo 3 : Múltiples Direcciones Públicas con Servidores Internos

En este ejemplo, existen 3 direcciones públicas asignadas por el ISP. Existen muchos departamentos pero dos disponen de su propio servidor FTP. Todos los departamentos comparten el mismo router. El ejemplo reservará una dirección pública para cada departamento con un servidor FTP y todos los departamentos utilizarán la otra dirección pública. Habrá que mapear los servidores FTP con las dos primeras direcciones públicas y el resto de tráfico de la LAN a la dirección pública restante. Mapear la tercera dirección pública a un servidor web y FTP interno. Se necesitarán configurar cuatro reglas, dos bidireccionales y dos unidireccionales, tal y como se indica a continuación.

Regla 1. Mapear la primera dirección pública al primer servidor FTP para habilitar el tráfico FTP en ambos sentidos (mapeo **1:1**, dando tanto la dirección privada como pública).

Regla 2. Mapear la segunda dirección pública al segundo servidor FTP interno habilitando el tráfico FTP en ambos sentidos (mapeo **1:1**, dando tanto la dirección privada como pública).

Regla 3. Mapear el resto de tráfico saliente de la LAN a la tercera dirección pública (mapeo **Many:1**).

Regla 4. También será necesario mapear la tercera dirección pública al servidor FTP y web en la LAN. El tipo **Server** permite especificar múltiples servidores, de tipos diferentes, a ordenadores de la LAN tras el NAT.

La situación del ejemplo se asemeja a lo que se muestra a continuación:

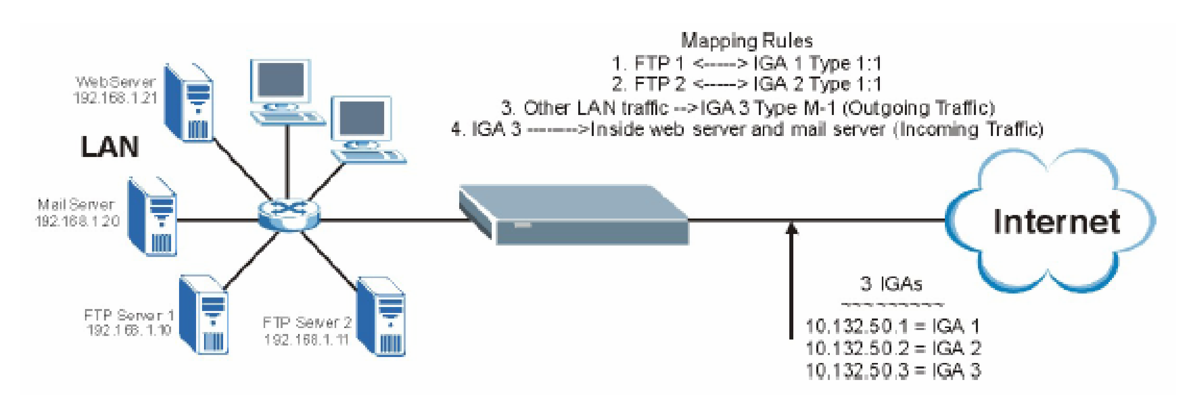


Figura 25-15 Ejemplo 3

Paso 1. En este caso será necesario configurar el conjunto 1 del mapeo de direcciones en el **Menu 15.1 – Address Mapping Sets**. Será necesario configurar la opción **Full Feature** en el campo **Network Address Translation** (en el menú 4 o menú 11.3) en la *Figura 29-16*.

Paso 2. Teclear 15 en el menú principal.

Paso 3. Introduzca 1 para configurar los Conjuntos de Mapeo de Direcciones.

Paso 4. Introduzca 1 para comenzar a configurar este nuevo conjunto. Introduzca un Nombre del Conjunto, escoja **Edit (Editar)** dentro del campo **Action (Acción)** y teclee 1 en el campo **Select Rule (Seleccionar Regla)**. Pulse [INTRO] para confirmar.

Paso 5. Seleccione el **Type (Tipo)** como **One-to-One** (mapeo directo de paquetes en ambos sentidos), e introducir la dirección IP Local de Inicio (**Local Start IP**) como 192.168.1.10 (la dirección IP del servidor FTP 1), la dirección de Inicio Global (**Global Start IP**) como 10.132.50.1 (la primera dirección pública). (ver *Figura 29-17*).

Paso 6. Repita los pasos previos para la configuración de las reglas 2 a 4.

Paso 7. Cuando finalice, el menú 15.1.1 debería aparecer como se muestra en la Figura 29-18.

```
                Menu 11.3 - Remote Node Network Layer Options

     IP Options:                         Bridge Options:
       IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
       Rem IP Addr: 0.0.0.0
       Rem Subnet Mask= 0.0.0.0
       My WAN Addr= 0.0.0.0
       NAT= Full Feature
         Address Mapping Set= 2
       Metric= 2
       Private= No
       RIP Direction= Both
         Version= RIP-2B
       Multicast= IGMP-v2
       IP Policies=

                   Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-16 Ejemplo 3 : Menu 11.3

Las siguientes figuras muestran como configurar la primera regla.

```
                    Menu 15.1.1.1 Address Mapping Rule

          Type= One-to-One

          Local IP:
            Start= 192.168.1.10
            End   = N/A

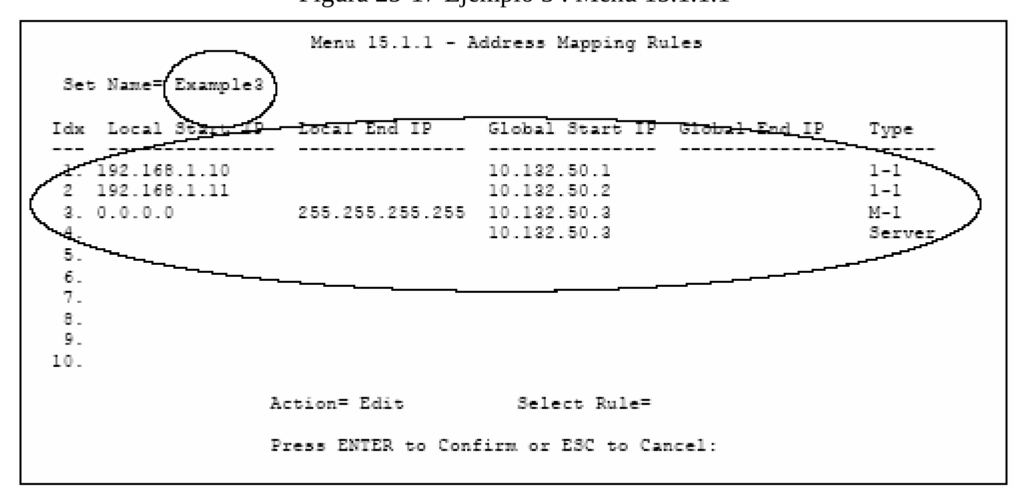
          Global IP:
            Start= 10.132.50.1
            End   = N/A

          Server Mapping Set= N/A


                          Press ENTER to Confirm or ESC to Cancel:

     Press Space Bar to Toggle.
```

Figura 25-17 Ejemplo 3 : Menu 15.1.1.1



```
                    Menu 15.1.1 - Address Mapping Rules

 Set Name= Example3

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1.  192.168.1.10                      10.132.50.1                       1-1
  2   192.168.1.11                      10.132.50.2                       1-1
  3.  0.0.0.0          255.255.255.255  10.132.50.3                       M-1
  4.                                    10.132.50.3                       Server
  5.
  6.
  7.
  8.
  9.
 10.

                    Action= Edit          Select Rule=

                    Press ENTER to Confirm or ESC to Cancel:
```

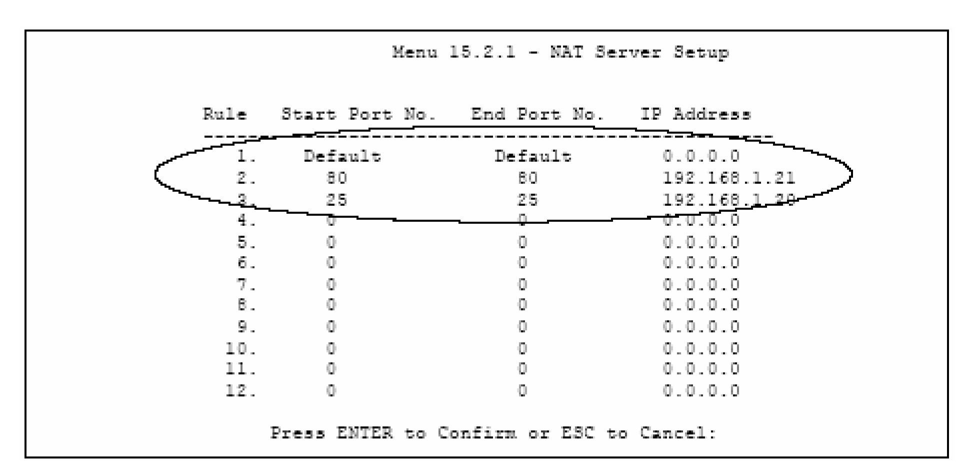
Figura 25-18 Ejemplo 3 : Menu 15.1.1.1 Final

Ahora habrá que configurar la tercera dirección pública para mapearla a nuestro servidor web y servidor de correo en la LAN.

Paso 8. Teclee 15 en el menú principal.

Paso 9. Introduzca 2 en el **Menu 15- NAT Setup**.

Paso 10. Introduzca 1 en el **Menu 15.2 – NAT Server Sets** para ver el siguiente menú. Configúrelo como se muestra.



```
                    Menu 15.2.1 - NAT Server Setup

        Rule   Start Port No.   End Port No.    IP Address
        ---------------------------------------------------
         1.      Default          Default         0.0.0.0
         2.      80               80              192.168.1.21
         3.      25               25              192.168.1.20
         4.      0                0               0.0.0.0
         5.      0                0               0.0.0.0
         6.      0                0               0.0.0.0
         7.      0                0               0.0.0.0
         8.      0                0               0.0.0.0
         9.      0                0               0.0.0.0
        10.      0                0               0.0.0.0
        11.      0                0               0.0.0.0
        12.      0                0               0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-19 Ejemplo 3 : Menu 15.2.1

25.5.4 Ejemplo 4 : Aplicaciones problemáticas con NAT

Algunas aplicaciones no soportan el mapeo NAT utilizando traslación de puertos TCP o UDP. En este caso es mejor utilizar un mapeo **Many-to-Many No Overload** dado que el número de puertos no varía para los tipos de mapeos **Many-to-Many No Overload** y **One-to-One**. La siguiente figura ilustra esto.

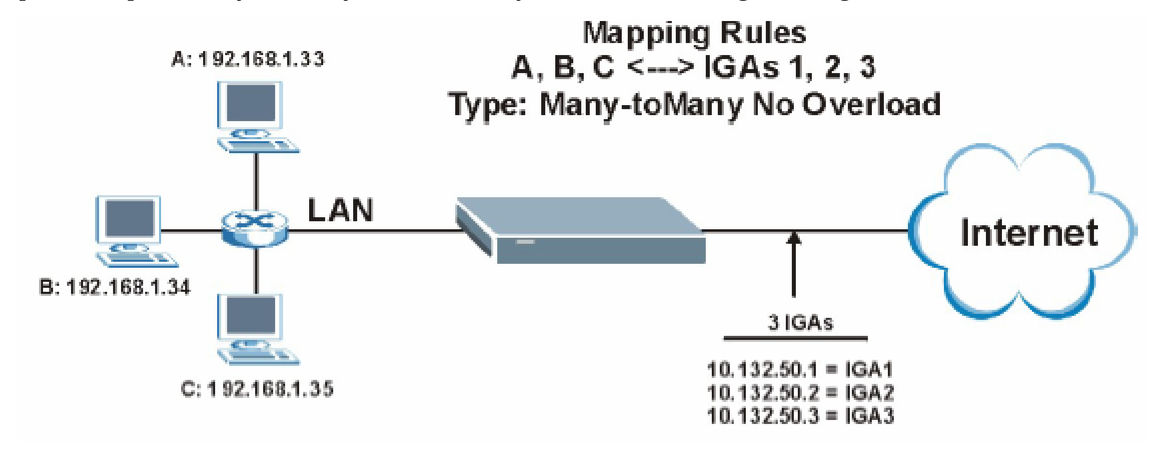


Figura 25-20 Ejemplo 4

Algunas otras aplicaciones tales como ciertos progrmas de juegos pueden presentar problemas con el NAT porque éstos incluyen información de direccionamiento en el stream de datos. Estas aplicaciones no trabajarán correctamente a través del NAT incluso aunque se utilicen tipos de mapeo **One-to-One** y

Many-to-Many No Overload.

Siga los pasos indicados en el ejemplo 3 para configurar estos dos menús como se indica.

```
                    Menu 15.1.1.1 Address Mapping Rule

     Type= Many-to-Many No Overload

     Local IP:
       Start= 192.168.1.10
       End  = 192.168.1.12

     Global IP:
       Start= 10.132.50.1
       End  = 10.132.50.3

     Server Mapping Set= N/A

                    Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-21 Ejemplo 4 : Menu 15.1.1.1 Regla de Mapeo de Direcciones

Después de haber configurado esta regla, debería ser capaz de visualizar los parámetros del menú 15.1.1 como se muestra.

```
                        Menu 15.1.1 - Address Mapping Rules

  Set Name= Example4

 Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
 ---  ---------------  ---------------  ---------------  ---------------  ------
  1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M:M NO OV
  2.
  3.
  4.
  5.
  6.
  7.
  8.
  9.
 10.
                   Action= Edit          Select Rule=

                   Press ENTER to Confirm or ESC to Cancel:
```

Figura 25-22 Ejemplo 4 : Menu 15.1.1 Reglas de Mapeo de Direcciones

Capítulo 26
Configuración del Filtrado

Este capítulo muestra como crear y aplicar los filtros.

26.1 Acerca del Filtrado

Su Prestige utiliza filtros para decidir si permitir o no el paso de paquetes de datos y/o realizar llamadas. Existen dos tipos de filtros de aplicaciones : filtros de datos y filtros de llamadas. Los filtros se subdividen en filtros de dispositivos y de protocolo, que se discutirán más tarde.

Las pantallas de los filtros de datos se utilizan para determinar si se debe dejar pasar o no un paquete. Los filtros de datos se dividen en filtros de entrada y de salida, dependiendo de la dirección de los paquetes relativos a un puerto. El filtrado de datos se puede aplicar bien en el lado WAN o en el lado Ethernet. El filtrado de llamadas se usa para determinar si se permite o no que un paquete pueda lanzar una llamada.

Los paquetes salientes deben pasar por el filtrado de datos antes de encontrarse con el filtrado de llamadas. El filtrado de llamadas se divide en dos grupos, el filtrado de llamadas ya implementado en el equipo y el definido por el usuario.El Prestige incluye filtros de llamada de prevención, como por ejemplo, que paquetes RIP puedan lanzar llamadas. Estos filtros están siempre habilitados y no son accesibles al usuario. El Prestige aplica los filtros integrados en primer lugar y a continuación los filtros de llamada definidos por el usuario, si están aplicables, como se indica a continuación.

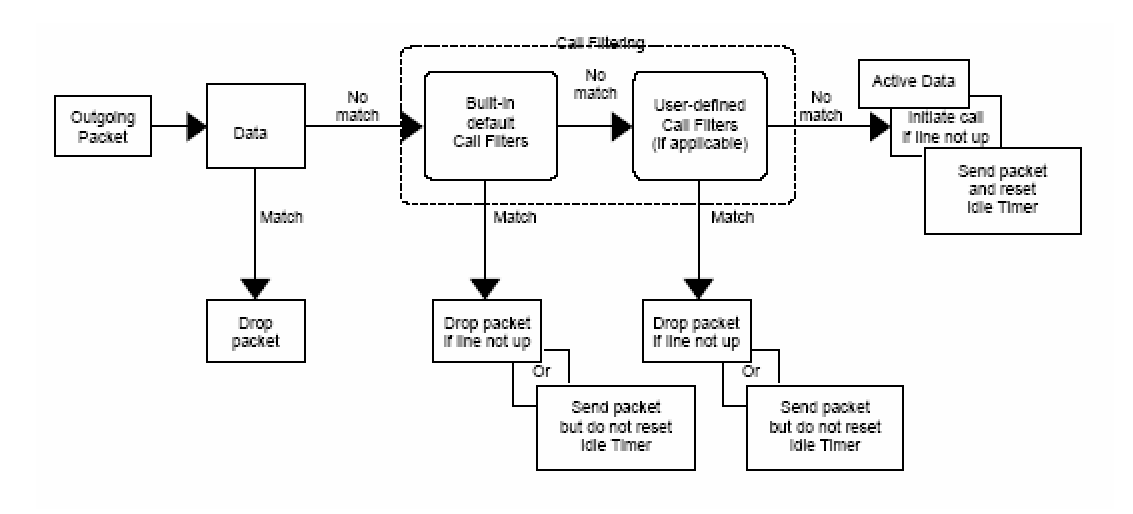


Figura 26-1 Proceso de Filtrado de Paquetes de Salida

Dos conjuntos de reglas de filtros de fábrica han sido configuradas en el menú 21 para prevenir que el tráfico NetBIOS puedan lanzar llamadas. Un resumen de estos filtros se muestra en las siguientes figuras.

La siguiente ilustración muestra el flujo lógico cuando se ejecuta una regla de filtrado.

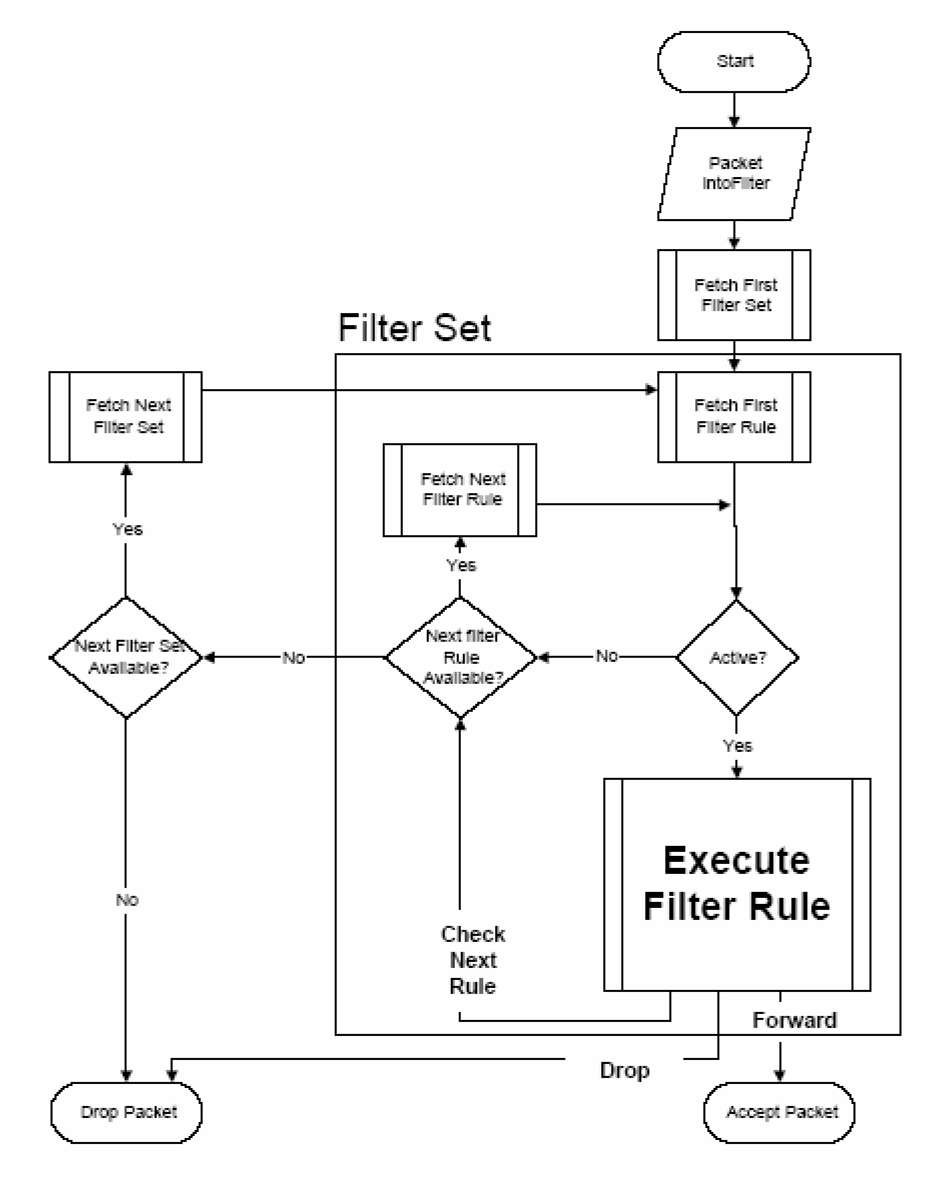


Figura 26-2 Proceso de una Regla de Filtrado

Se pueden aplicar hasta cuatro conjuntos de filtros a un puerto en particular para bloquear varios tipos de paquete. Como cada filtro puede contener hasta 6 reglas, se pueden tener como máximo 24 reglas activas por puerto.

Para los paquetes entrantes, el Prestige aplica únicamente filtros de datos. Los paquetes son procesados dependiendo de si se encuentra o no coincidencia. La siguiente sección describe como configurar los conjuntos de filtros.

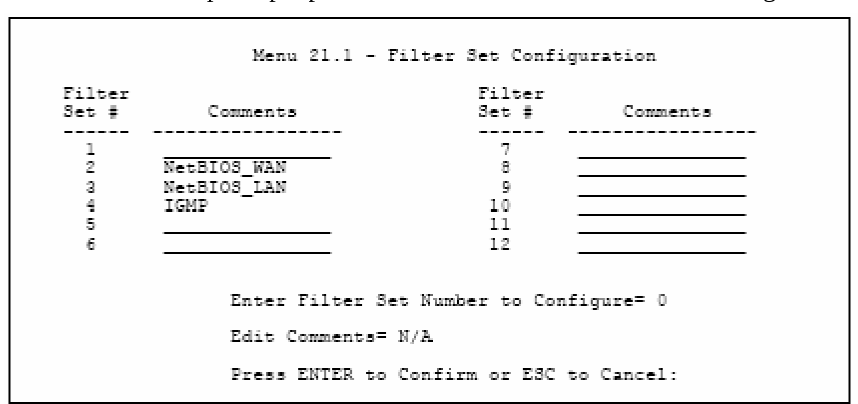
La estructura del Filtro en el Prestige

Un filtro consiste en una o más reglas. Normalmente, se deben agrupar las reglas relacionadas, por ejemplo, todas las reglas relativas al NetBIOS en un único conjunto y darle un nombre descriptivo. Se pueden configurar hasta 12 conjuntos de filtros con 6 reglas por cada uno, lo que da un total de 72 reglas de filtrado configurables en el sistema.

26.2 Configuración de un Filtro en el Prestige

Para configurar un filtro, siga los siguientes pasos.

Paso 1. Teclee 21en el menú principal para mostrar el Menu 21 – Filter Set Configuration.



```
                    Menu 21.1 - Filter Set Configuration

  Filter                                    Filter
  Set #        Comments                     Set #        Comments
  ------  -----------------                 ------  -----------------
    1     _______________                     7     _______________
    2     NetBIOS_WAN                         8     _______________
    3     NetBIOS_LAN                         9     _______________
    4     IGMP                               10     _______________
    5     _______________                    11     _______________
    6     _______________                    12     _______________

                 Enter Filter Set Number to Configure= 0

                 Edit Comments= N/A

                 Press ENTER to Confirm or ESC to Cancel:
```

Figura 26-3 Menu 21 Configuración del Filtro

Paso 2. Introduzca el conjunto de filtrado a configurar (no.1 al 12) y presione [INTRO].

Paso 3. Introduzca un nombre descriptivo o comentario en el campo **Edit Comments** y presione [INTRO].

Paso 4. Pulse [INTRO] en la línea de mensaje “Press ENTER to confirm…” para mostrar el **Menu 21.1 – Filter Rules Summary** (esto es, si se seleccionó el conjunto de filtrado 1 en el menú 21.).

```
                          Menu 21.1.2 - Filter Rules Summary

 # A Type                        Filter Rules                                M m n
 - - ---- --------------------------------------------------------------- - - -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                          N D N
 2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                          N D N
 3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                          N D N
 4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                         N D N
 5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                         N D N
 6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                         N D F


                    Enter Filter Rule Number (1-6) to Configure:
```

Figura 26-4 Resumen de las Reglas de Filtrado NetBIOS_WAN

```
                          Menu 21.1.3 - Filter Rules Summary

 # A Type                        Filter Rules                                M m n
 - - ---- --------------------------------------------------------------- - - -
 1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                  N D F
 2 N
 3 N
 4 N
 5 N
 6 N
                    Enter Filter Rule Number (1-6) to Configure:
```

Figura 26-5 Resumen Reglas de Filtrado NetBIOS_LAN

```
                          Menu 21.1.4 - Filter Rules Summary

 # A Type                        Filter Rules                                M m n
 - - ---- --------------------------------------------------------------- - - -
 1 Y Gen  Off=0, Len=3, Mask=ffffff, Value=01005e                        N D F
 2 N
 3 N
 4 N
 5 N
 6 N


                    Enter Filter Rule Number (1-6) to Configure:
```

Figura 26-6 Resumen Reglas de Filtrado IGMP

26.3 Menús Resumen de Reglas de Filtrado

Las siguientes tablas describen de forma resumida las abreviaturas utilizadas en los menús 21.1.1 y 21.1.2.

Tabla 26-1 Abreviaturas utilizadas en los Menús de Resumen de las Reglas de Filtrado

CAMPO	DESCRIPCIÓN
#	El número de la regla del filtro: 1 a 6
A	Active : "Y" indica que la regla está activa. "N" indica que la regla está inactiva.
Type	El tipo de la regla del filtro : "GEN" para filtro genérico, "IP" para filtro TCP/IP.
Filter Rules	Estos parámetros se muestran aquí.
M	More (Más). "Y" significa que hay más reglas a chequear formando una cadena de reglas con la regla actual. No se podrá tomar ninguna acción hasta que se haya completado la cadena. "N" indica que no existen más reglas para chequear. Es posible especificar una acción a llevar a cabo, por ejemplo, el envío del paquete, el descarte del paquete o el chequeo de la siguiente regla. Para la última, la siguiente regla es independiente de la regla recién comprobada.
m	Action Matched (Acción cuando hay coincidencia). "F" significa enviar el paquete inmediatamente y pasar de comprobar las reglas restantes. "D" indica que hay que descartar el paquete. "N" indica que hay que comprobar la siguiente regla.
n	Action Not Matched (Acción cuando no hay coincidencia). "F" significa enviar el paquete inmediatamente y pasar de comprobar las reglas restantes. "D" indica que hay que descartar el paquete. "N" indica que hay que comprobar la siguiente regla.

Las abreviaturas de las reglas de filtrado dependientes del protocolo se listan a continuación:

Tabla 26-2 Abreviaturas de Regla Utilizadas

TIPO DE FILTRO	DESCRIPCIÓN
IP	
Pr	Protocolo

SA	Source Address (Dirección Origen)
SP	Source Port Number (Número de Puerto Origen)
DA	Destination Address (Dirección Destino)
DP	Destination Port Number (Número de Puerto Destino)
GEN	
Off	Offset (Desplazamiento)
Len	Length (Longitud)

26.4 Configuración de una Regla de Filtrado

Para configurar una regla de filtrado, introduzca su número en el **Menu 21.1.x –Filter Rules Summary** y pulse sobre [INTRO] para abrir el menú 21.x 1 para la regla.

Existen dos tipos de reglas de filtrado : **TCP/IP** y **Generic**. En función del tipo de regla, los parámetros a configurar para cada tipo serán diferentes. Utilice la [BARRA ESPACIADORA] para seleccionar el tipo de regla que desea crear en el campo **Filter Type** y presione [INTRO] para abrir el menú respectivo.

Para acelerar el filtrado, todas las reglas de un conjunto deberán ser de la misma clase, por ejemplo, filtros de protocolo o filtros genéricos. La clase del conjunto de filtrado se determina por la primera regla que se crea. Cuando se aplican los conjuntos de filtrado a un puerto, se presentan campos separados para aplicar los conjuntos de filtros de protocolo y de dispositivo (genéricos). Si se incluye un conjunto de filtrado de protocolo en un campo dedicado a aplicar filtros de dispositivos o viceversa, el Prestige dará un aviso de este hecho y no permitirá almacenar los cambios.

26.4.1 Regla de Filtrado TCP/IP

Esta sección muestra como configurar una regla de filtrado TCP/IP. Las reglas TCP/IP permiten basar la regla en los campos de la cabecera del protocolo IP y superiores, por ejemplo, cabeceras TCP y UDP.

Para configurar las reglas TCP/IP, seleccione TCP/IP Filter Rule en el campo **Filter Type** y presione [INTRO] para abrir el Menu 21.1.x.1 – TCP/IP Filter Rule, como se indica.

```
                    Menu 21.1.1.1 - TCP/IP Filter Rule

                Filter #: 1,1
                Filter Type= TCP/IP Filter Rule
                Active= No
                IP Protocol= 0     IP Source Route= No
                Destination: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                     Source: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                TCP Estab= N/A
                More= No            Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

                Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figura 26-7 Menu 21.1.x.1 Regla de Filtrado TCP/IP

La siguiente tabla describe como configurar la regla de filtrado TCP/IP.

Tabla 26-3 Menu 21.1.x.1 Relga de Filtrado TCP/IP

CAMPO	DESCRIPCIÓN	EJEMPLO
Destination:		
IP Addr	Introduzca la dirección IP destino del paquete que se desea filtrar. El campo es ignorado si se coloca a 0.0.0.0	Dirección IP
IP Mask	Introduzca la máscara IP a aplicar a la dirección destino anterior.	Máscara IP
Port #	Introduzca el puerto destino de los paquetes que se desean filtrar. El rango del campo es de 0 a 65535. Un campo a 0 es ignorado.	0 a 65535
Port # Comp	Seleccione la comparación que se aplicará al puerto destino en el paquete frente al valor dado en Destination : Port #. Las opciones son **None (Ninguno), Less (Menor), Greater(Mayor), Equal(Igual)** o **Not Equal(Desigual).**	None
Source:		
IP Addr	Introduzca la dirección IP origen del paquete que se desea filtrar. El campo es ignorado si se coloca a 0.0.0.0	Dirección IP
IP Mask	Introduzca la máscara IP a aplicar a la dirección origen anterior.	Máscara IP

Port #	Introduzca el puerto origen de los paquetes que se desean filtrar. El rango del campo es de 0 a 65535. Un campo a 0 es ignorado.	0 a 65535
Port # Comp	Seleccione la comparación que se aplicará al puerto origen en el paquete frente al valor dado en Source : Port #. Las opciones son **None (Ninguno), Less (Menor), Greater(Mayor), Equal(Igual)** o **Not Equal(Desigual).**	None
TCP Estab	Esto se aplica únicamente cuando el campo del Protocolo IP es 6, TCP. Si está a Yes, la regla coincide con los paquetes que quieren establecer conexiones TCP (SYN=1 y ACK=0); en cualquier otro caso es ignorado.	No (por defecto)
More	Si está a **Yes**, un paquete que coincida se pasa a la siguiente regla de filtrado antes de tomar una acción o en otro caso el paquete se pasa por la correspondiente acción configurada en el campo de acción. Si **More** está a **Yes**, entonces los campos **Action Matched** y **Action Not Matched** se colocan en N/A.	No (por defecto)
Log	Seleccione las opciones de captura de logs entre las siguientes: **None** – No registrar ningún paquete **Action Matched** – Sólo registrar paquetes que coincidan con los parámetros de la regla **Action Not Matched –** Sólo registrar los paquetes que no coincidan con los parámetros de la regla. **Both –** Registrar todos los paquetes.	None
Action Matched	Seleccione la acción a tomar cuando exista coincidencia. Las opciones son **Check Next Rule (Comprobar la Siguiente Regla), Forward (Dejar Pasar)** o **Drop (Descartar).**	Check Next Rule (por defecto)
Action Not Matched	Seleccione la acción a tomar cuando no exista coincidencia. Las opciones son Check **Next Rule (Comprobar la Siguiente Regla), Forward (Dejar Pasar)** o **Drop (Descartar).**	Check Next Rule (por defecto)
Cuando haya completado este menú, presione [INTRO] en la línea de mensaje “Press ENTER to confirm…” para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla anterior.		

La siguiente figura ilustra el flujo lógico de un filtro IP.

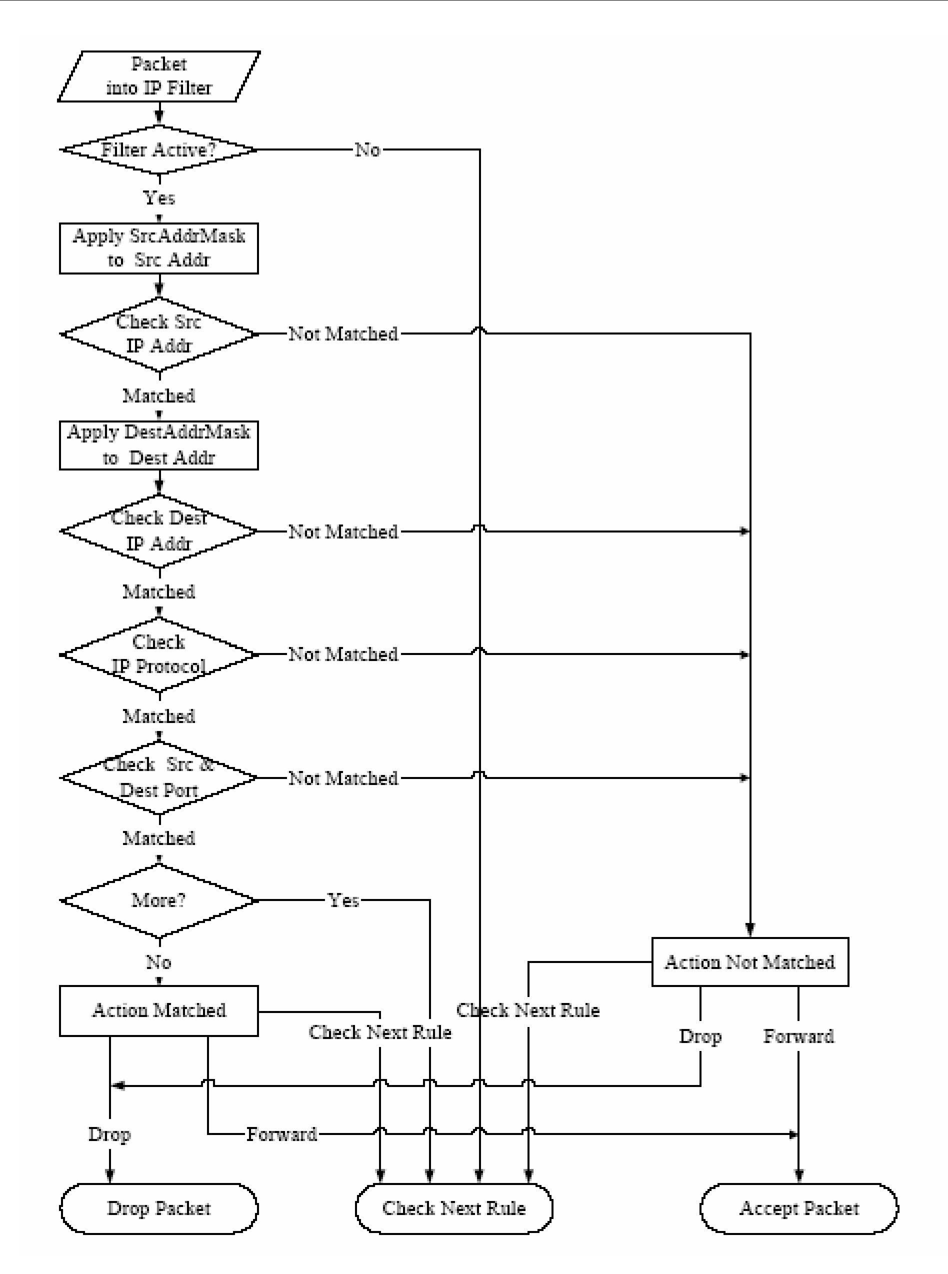


Figura 26-8 Ejecución de un Filtro IP

26.4.2 Regla de Filtrado Genérico

Esta sección muestra como configurar una regla de filtrado genérica. La finalidad de estas reglas genéricas es permitir el filtrado de paquetes no-IP. Para IP, es normalmente más sencillo utilizar reglas IP directamente.

Para las reglas genéricas, el Prestige trata un paquete como una cadena de bytes en contraposicón a un paquete IP. Se especifica la porción del paquete a chequear a través de los campos **Offset (Desplazamiento)** (desde 0) y **Length (Longitud),** ambos en bytes. El Prestige aplica la máscara a la porción de datos antes de comparar el resultado frente al valor para determinar la coincidencia. Los campos **Mask (Máscara)** y **Value (Valor)** se especifican con números hexadecimales. Indicar que se necesitan dos dígitos hexadecimales para representar un byte, así que si la longitud es 4, el valor en cualquier campo será de 8 dígitos, por ejemplo, FFFFFFFF.

Para configurar una regla genérica seleccione un conjunto de filtrado vacía en el menú 21, por ejemplo, la 5. Seleccione **Generic Filter Rule** en el campo **Filter Type** y presione [INTRO] para abrir el **Menu 21.1.5.1 – Generic Filter Rule**, como se muestra en la siguiente figura.

```
                    Menu 21.1.5.1 - Generic Filter Rule

                  Filter #: 5,1
                  Filter Type= Generic Filter Rule
                  Active= No
                  Offset= 0
                  Length= 0
                  Mask= N/A
                  Value= N/A
                  More= No           Log= None
                  Action Matched= Check Next Rule
                  Action Not Matched= Check Next Rule

                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figura 26-9 Menu 21.1.5.1 Regla de Filtrado Genérica

La siguiente tabla describe los campos en el menú de la Regla de Filtrado Genérica.

Tabla 26-4 Menu 21.1.5.1 Regla de Filtrado Genérica

CAMPO	DESCRIPCIÓN	EJEMPLO
Filter #	Éste es el conjunto del filtro, regla de filtrado, por ejemplo, 2,3 hace referencia al segundo conjunto de filtros y a la tercera regla de ese conjunto	5,1
Filter Type	Presione [BARRA ESPACIADORA] y a continuación [INTRO] para seleccionar el tipo de la regla. Los parámetros que se muestran más abajo	Generic Filter Rule

	serán diferentes para cada tipo de filtro. Las opciones son **Generic Filter Rule** o **TCP/IP Filter Rule**.	
Active	Seleccione Yes para activar o No para desactivar la regla.	No (por defecto)
Offset	Introduzca el byte de comienzo de la porción de datos del paquete que desea comparar. El rango de este campo va desde 0 a 255.	0 (por defecto)
Length	Introduzca el contador de bytes de la porción de datos del paquete que desea comparar. El rango de este campo va de 0 a 8.	0 (por defecto)
Mask	Introduzca la máscara (en formato hexadecimal) a aplicar a la porción de datos antes de la comparación.	
Value	Introduzca el valor (en formato hexadecimal) a comparar con la porción de datos.	
More	Si está a **Yes**, un paquete que coincida se pasa a la siguiente regla de filtrado antes de tomar una acción o en otro caso el paquete se pasa por la correspondiente acción configurada en el campo de acción. Si **More** está a **Yes**, entonces los campos **Action Matched** y **Action Not Matched** se colocan en N/A.	No (por defecto)
Log	Seleccione las opciones de captura de logs entre las siguientes: **None –** No registrar ningún paquete **Action Matched –** Sólo registrar paquetes que coincidan con los parámetros de la regla **Action Not Matched** – Sólo registrar los paquetes que no coincidan con los parámetros de la regla. **Both –** Registrar todos los paquetes.	None
Action Matched	Seleccione la acción a tomar cuando exista coincidencia. Las opciones son **Check Next Rule (Comprobar la Siguiente Regla), Forward (Dejar Pasar)** o **Drop (Descartar).**	Check Next Rule (por defecto)
Action Not Matched	Seleccione la acción a tomar cuando no exista coincidencia. Las opciones son Check **Next Rule (Comprobar la Siguiente Regla), Forward (Dejar Pasar)** o **Drop (Descartar).**	Check Next Rule (por defecto)
Cuando haya completado este menú, presione [INTRO] en la línea de mensaje “Press ENTER to confirm…” para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla anterior.		

26.5 Tipos de Filtros y NAT

Existen dos clases de reglas de filtrado, reglas de Filtrado de Dispositivo (Genéricas) y reglas de Filtrado de Protocolo (TCP/IP). Las reglas de filtrado genéricas actúan sobre los datagramas desde/hacia la LAN y WAN. Las reglas de filtrado de protocolo actúan sobre los paquetes IP.

Cuando el NAT (Network Address Translation) está habilitado, la dirección IP interna y el número de puerto son reemplazados, lo que hace imposible conocer la dirección y el puerto exactos en el par. Por lo tanto, el Prestige aplica el filtrado de protocolo a la dirección IP y el puerto “nativos” antes del NAT para los paquetes salientes y tras el NAT a los paquetes entrantes. Por otro lado, los filtros genéricos se aplican al flujo de paquetes que aparecen sobre el hilo. Éstos son aplicados en el punto en el que el Prestige está enviando y recibiendo los paquetes; por ejemplo, el interfaz. El interfaz puede ser un Ethernet, o cualquier otro puerto hardware. La siguiente figura ilustra esto.

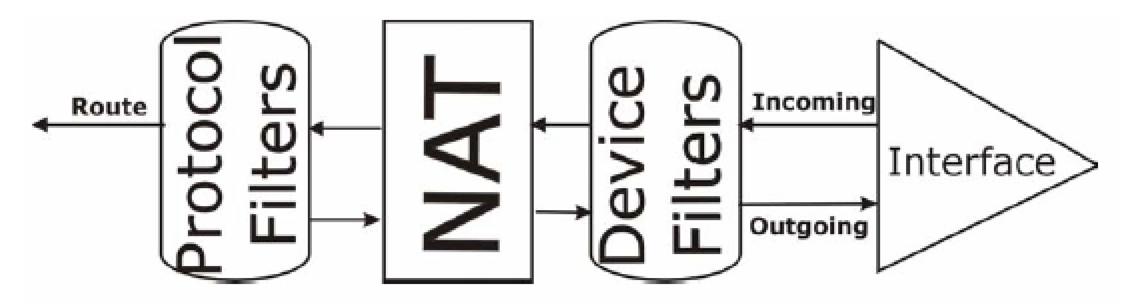


Figura 26-10 Filtros de Protocolo y Dispositivo

26.6 Ejemplo de Filtro

Vamos a ver un ejemplo para bloquear a los usuarios externos el acceder via telnet al Prestige.

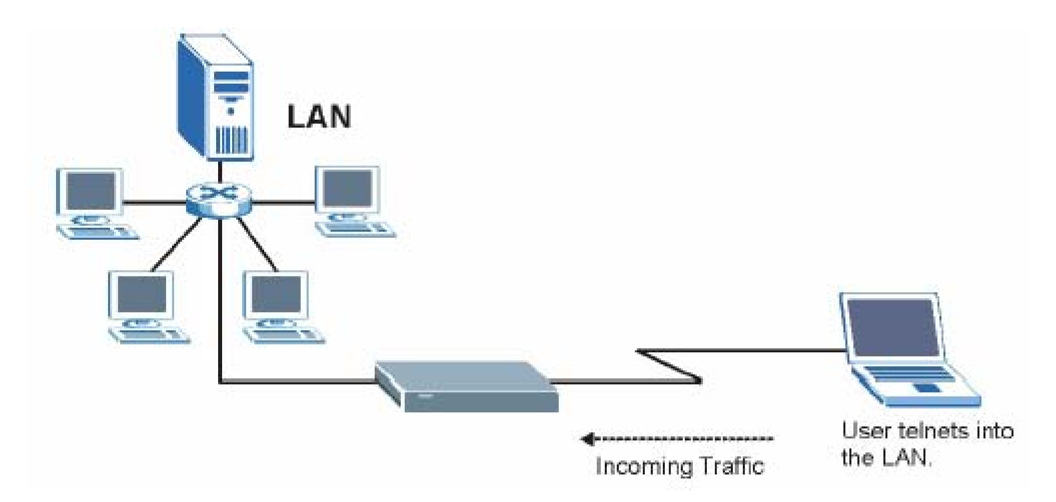


Figura 26-11 Ejemplo de Filtro Telnet

Paso 1. Teclee 1 en el menu 21 para mostrar el **Menu 21.1 – Filter Set Configuration**.

Paso 2. Introduzca el número de índice del conjunto de filtrado que se desea configurar (en este caso el 6).

Paso 3. Teclee un nombre desciptivo o comentario en el campo **Edit Comments** (por ejemplo, TELNET_WAN) y pulse [INTRO].

Paso 4. Pulse [INTRO] en la línea de mensaje "Press [ENTER] to confirm…" para abrir el **Menu 21.1.6 – Filter Rules Summary**.

Paso 5. Introduzca 1 para configurar la primera regla de filtrado.

Cuando se presione [INTRO] para confirmar, aparecerá la siguiente pantalla. Indicar que únicamente habrá una regla de filtrado en este conjunto.

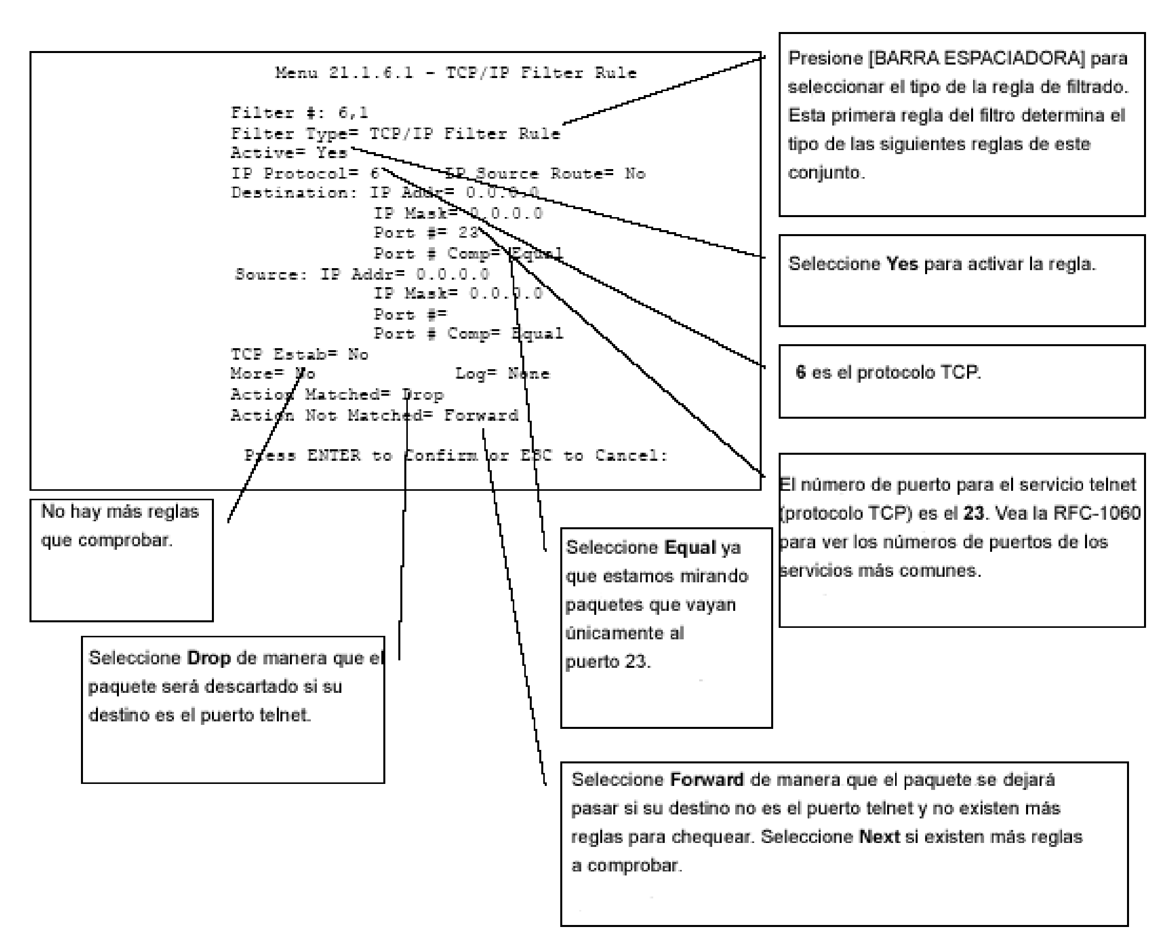


Figura 26-12 Menu 21.1.6.1 Filtro de Ejemplo

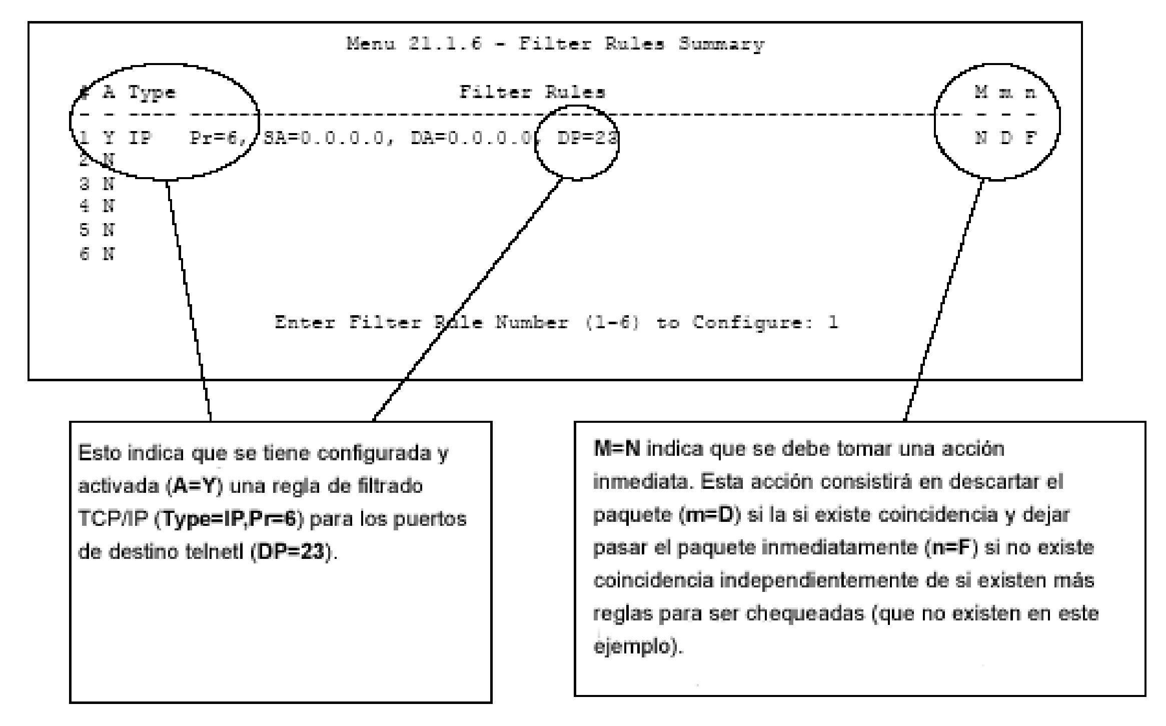


Figura 26-13 Menu 21.1.6.1 Resumen Regla de Ejemplo

Tras haber creado el filtro, será necesario aplicarlo.

Paso 1. Teclee 11 en el menú principal para mostrar el menú 11 e introduzca el número de nodo remoto para editarlo.

Paso 2. Vaya al campo **Edit Filter Sets**, presione [BARRA ESPACIADORA], seleccione **Yes** y pulse [INTRO].

Paso 3. Esto mostrará el menú 11.5. Aplique el filtro de ejemplo (por ejemplo, el filtro 3) en este menú como se indica en la siguiente sección.

26.7 Aplicación de Filtros y Filtros por Defecto

Esta sección muestra como aplicar el filtro o filtros tras haberlo(s) diseñado. Los filtros por defecto han sido configurados en el menú 21 (pero no ha sido aplicados todavía) para filtrar cierto tráfico.

Tabla 26-5 Tabla de Conjuntos de Filtrado

CONJUNTOS DE FILTRADO	DESCRIPCIÓN
Input Filter Sets:	Aplica los filtros al tráfico entrante. Es necesario aplicar reglas de filtrado de protocolo o dispositivo. Vaya a las secciones anteriores para obtener más información al respecto.
Output Filter Sets:	Aplica los filtros al tráfico saliente. Es necesario aplicar reglas de filtrado de protocolo o dispositivo. Vaya a las secciones anteriores para obtener más información al respecto.
Call Filter Sets:	Aplica los filtros para decidir si a un paquete le está permitido lanzar una llamada.

26.7.1 Tráfico Ethernet

Raramente será necesario filtrar el tráfico Ethernet; sin embargo, los filtros pueden ser útiles para bloquear determinados paquetes, reducir tráfico y prevenir agujeros de seguridad. Vaya al menú 3.1 (mostrado a continuación) e introduzca el número o números de los filtros que se desean aplicar. Se pueden seleccionar hasta cuatro filtros (de doce) introduciendo sus números separados por comas, por ejemplo, 3,4,6,11. El filtro configurado por defecto, NetBIOS_LAN, puede ser insertado en el campo **protocol filters** bajo en epígrafe **Input Filter Sets** en el menú 3.1 para prevenir que los mensajes NetBIOS puedan lanzar llamadas al servidor DNS.

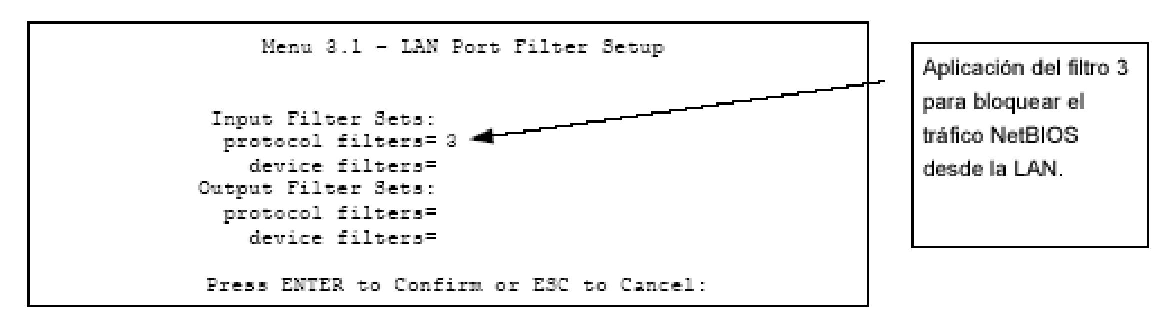


Figura 26-14 Filtrado del Tráfico Ethernet

26.7.2 Filtros en Nodos Remotos

Vaya al menú 11.5 (mostrado a continuación) e introduzca el número o números de filtros. Se pueden colocar en cascada hasta 4 filtros introduciendo sus números separado por comas. El filtro configurado por

defecto, NetBIOS_WAN, puede ser insertado en el campo **protocol filters** bajo el epígrafe **Call Filter Sets** en el menú 11.5 para bloquear que el tráfico NetBIOS local pueda lanzar llamadas al ISP.

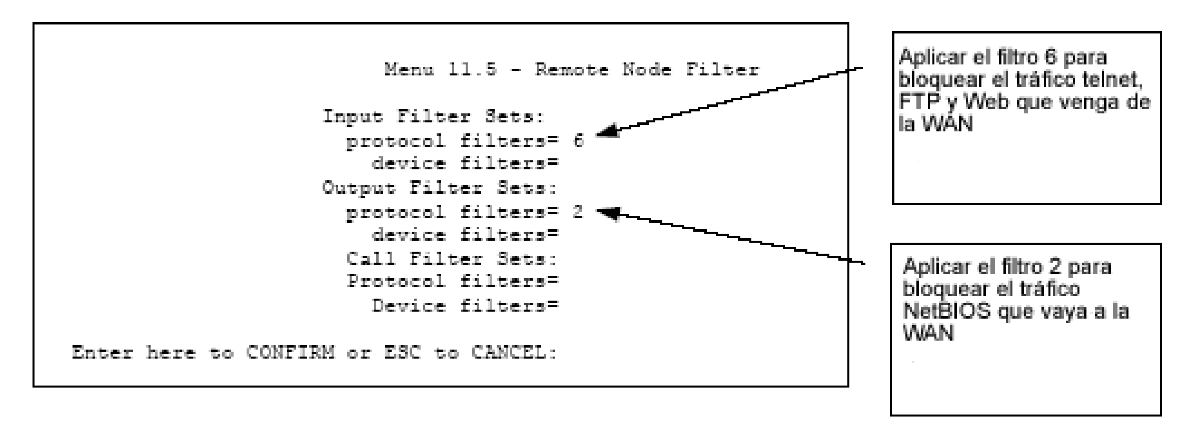


Figura 26-15 Filtrado de Tráfico en el Nodo Remoto

Indicar que el filtrado de llamadas están visibles cuando se selecciona la encapsulación PPPoA o PPPoE.

Capítulo 27
Configuración SNMP

Este capítulo explica la configuración SNMP del menú 22.

27.1 Acerca del SNMP

SNMP (Simple Network Management Protocol – Protocolo de Gestión de Red Simple) es un protocolo utilizado para intercambiar información de gestión entre dispositivos de red. SNMP es un miembro del conjunto de protocolos TCP/IP. El Prestige soporta la funcionalidad de agente SNMP, lo que permite a una máquina de gestión el controlar y monitorizar el Prestige a través de la red. El Prestige soporta la versión 1 SNMP (SNMPv1) y la versión dos c (SNMPv2c). La siguiente figura ilustra una operación de gestión SNMP. SNMP únicamente estará disponible si el TCP/IP está configurado.

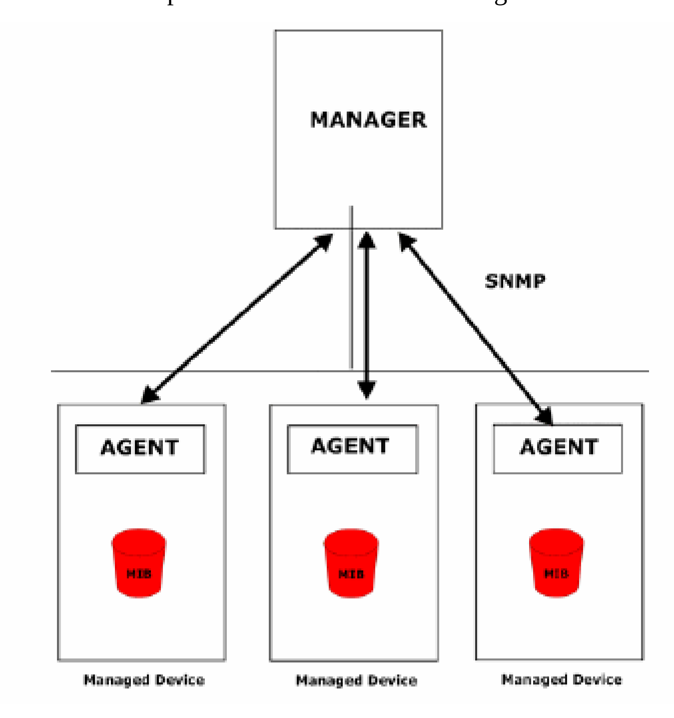


Figura 27-1 Modelo de Gestión SNMP

Una red gestiona SNMP consiste en dos componentes principales : agentes y un gestor.

Un agente es un módulo software de gestión que reside en un dispositivo gestionado (el Prestige). Un agente traduce la información de gestión local del dispositivo gestionado a una forma compatible con SNMP. El administrador es la consola a través de la cual los administradores de red llevan a cabo las funciones de gestión de la red. Ejecuta aplicaciones que controlan y monitorizan los dispositivos gestionados.

Los dispositivos gestionados contienen variables objeto que definen cada parte de información que será recogida sobre un dispositivo. Ejemplos de variables serían el número de paquetes recibidos, el estado del puerto del nodo, etc. Una base de información de gestión (Management Information Base, MIB) es un conjunto de variables objeto. SNMP permite al administrador y a los agentes comunicarse para acceder a estos objetos.

SNMP en sí mismo es un simple protocolo petición/respuesta basado en el modelo administrador/agente. El administrador emite una petición y el agente da una respuesta a través del siguiente protocolo de operaciones:

- Get - Permite al administrador recuperar una variable objeto del agente.
- GetNext – Permite al administrador recuperar la siguiente variable objeto de una tabla o lista dentro de un agente. En SNMPv1, cuando un administrador quiere recuperar todos los elementos de una tabla de un agente, empieza con una operación Get, seguida de una serie de operaciones GetNext.
- Set – Permite al administrador configurar valores para las variables dentro de un agente.
- Trap - Usado por el agente para informar al administrador sobre algunos eventos.

27.2 MIBs Soportadas

El Prestige soporta RFC-1215 y MIB II como se define en la RFC-1213 así como las MIBs privadas de ZyXEL. El foco de las MIBs es permitir a los administradores el recoger datos estadísticos y monitorizar el estado y funcionamiento.

27.3 Configuración SNMP

Para configurar el SNMP, seleccione la opción 22 del menú principal para abrir el **Menu 22 – SNMP Configuration** como se muestra seguidamente. La “community” para los campos Get, Set y Trap es la terminología utilizada por el SNMP para la contraseña.

```
                Menu 22 - SNMP Configuration

          SNMP:
            Get Community= public
            Set Community= public
            Trusted Host= 0.0.0.0
            Trap:
              Community= public
              Destination= 0.0.0.0


            Press ENTER to Confirm or ESC to Cancel:
```

Figura 27-2 Menú 22 Configuración SNMP

La siguiente tabla describe los parámetros de configuración SNMP.

Tabla 27-1 Menu 22 Configuración SNMP

CAMPO	DESCRIPCIÓN	EJEMPLO
SNMP:		
Get Community	Introduzca la **Get Community**, que es la contraseña para las peticiones entrantes Get y GetNext que vienen de la estación de administración.	public
Set Community	Introduzca la **Set Community**, que es la contraseña para las peticiones entrantes Set provinientes de la estación de administración.	public
Trusted Host	Si introduce un host seguro, el Prestige solamente responderá a los mensajes SNMP que vengan de esta dirección. Dejar el campo en blanco (opción por defecto) significa que el Prestige responderá a todos los mensajes SNMP que le lleguen, sin importar su origen.	0.0.0.0
Trap:		
Community	Introduzca la **trap community**, que es la contraseña enviada con cada sentencia al administrador SNMP.	public
Destination	Teclee la dirección IP de la estación a la que va a enviar los SNMP traps.	0.0.0.0
Cuando haya completado este menú, pulse [ENTER] cuando aparezca el mensaje “Press ENTER to confirm or ESC to cancel” para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla anterior.		

27.4 Traps SNMP

El Prestige enviará traps al gestor SNMP cuando se produzca alguno de los siguientes eventos:

Tabla 27-2 Traps SNMP

TRAP #	NOMBRE TRAP	DESCRIPCIÓN
1	coldStart (definido en RFC-1215)	Se envía un trap después de iniciar (encendido).
2	warmStart (definido en RFC-1215)	Se envía un trap después de reiniciar (reinicio de software).
3	linkDown (definido en RFC-1215)	Trap que se envía con el número de puerto cuando cualquier de los enlaces está caído. Vea la siguiente tabla.
4	linkUp (definido en RFC-1215)	Se envía un trap con el número de puerto.
5	authenticationFailure (definido en RFC-1215)	Se envía un trap al administrador cuando se recive un SNMP get o set con la comunidad (contraseña) errónea.
6	whyReboot (definido en RFC-1215)	Se envía un trap con la razón del reinicio antes de que el sistema vaya a reiniciarse (inicio en caliente).
6a	For intentional reboot:	Se envía un trap con el mensaje “System reboot by user!” si el reinicio se hace intencionadamente, (por ejemplo, descarga de nuevos ficheros, Comando “sys reboot”, etc.).

El número de puerto es el índice del interfaz bajo el grupo de interfaz.

Tabla 27-3 Puertos y Circuitos Virtuales Permanentes

PUERTO	PVC (CIRCUITO VIRTUAL PERMANENTE)
1	Ethernet LAN
2	1
3	2
….	….
13	12
14	xDSL

Capítulo 28
Seguridad del Sistema

Este capítulo describe como configurar la seguridad del sistema en el Prestige.

28.1 Seguridad del Sistema

Es posible configurar la contraseña del sistema, un servidor RADIUS externo y la autenticación 802.1x en el menú 23.

28.1.1 Contraseña del Sistema

Teclee 23 en el menú principal para mostrar el **Menu 23 – System Security**.

Sería recomendable modificar la contraseña por defecto. Si olvida su contraseña sería necesario restaurar los parámetros de fábrica en el dispositivo. Consulte la sección acerca de la modificación de la contraseña del sistema en el capítulo de *Introducción al SMT* y la sección sobre el reseteo del Prestige en el capítulo *Introducción al Configurador Web*.

```
Menu 23 - System Security

     1. Change Password
     2. RADIUS Server

     4. IEEE802.1x
```

Figura 28-1 Menu 23 Seguridad del Sistema

28.1.2 Configuración de un Servidor RADIUS Externo

Desde el **Menu 23 – System Security**, teclee 2 para mostrar el **Menu 23.2 – System Security – RADIUS Server**.

```
Menu 23 - System Security

     1. Change Password
     2. RADIUS Server

     4. IEEE802.1x
```

Figura 28-2 Menu 23 Seguridad del Sistema

```
Menu 23.2 - System Security - RADIUS Server

 Authentication Server:
   Active= No
   Server Address= 10.11.12.13
   Port #= 1812
   Shared Secret= ********

 Accounting Server:
   Active= No
   Server Address= 10.11.12.13
   Port #= 1813
   Shared Secret= ********


 Press ENTER to Confirm or ESC to Cancel:
```

Figura 28-3 Menu 23.2 Seguridad del Sistema : Servidor RADIUS

La siguiente tabla describe los campos de este menú.

Tabla 28-1 Menu 23.2 Seguridad del Sistema : Servidor RADIUS

CAMPO	DESCRIPCIÓN	EJEMPLO
Authentication Server		
Active	Presione [BARRA ESPACIADORA] para seleccionar **Yes** y pulse [INTRO] para habilitar la autenticación de usuario a través del servidor de autenticación externo.	No
Server Address	Introduzca la dirección IP del servidor externo de autenticación en formato decimal.	10.11.12.13
Port	El puerto por defecto del servidor RADIUS de autenticación es el **1812**. No será necesario modificar este valor a menos que el administrador de red proporcione información adicional.	1812
Shared Secret	Especifique la contraseña (hasta 31 caracteres alfanuméricos) como la clave que será compartida entre el servidor de autenticación externo y los puntos de acceso. La clave no se envía a través de la red. Esta clave debe ser la misma en el servidor externo de autenticación y el Prestige.	
Accounting Server		
Active	Presione [BARRA ESPACIADORA] para seleccionar **Yes** y pulse [INTRO] para habilitar la contabilidad de usuario a	No

	través del servidor de contabilidad externo.	
Server Address	Introduzca la dirección IP del servidor externo de contabilidad en formato decimal.	10.11.12.13
Port	El puerto por defecto del servidor RADIUS de contabilidad es el **1813**. No será necesario modificar este valor a menos que el administrador de red proporcione información adicional.	1813
Shared Secret	Especifique la contraseña (hasta 31 caracteres alfanuméricos) como la clave que será compartida entre el servidor de contabilidad externo y los puntos de acceso. La clave no se envía a través de la red. Esta clave debe ser la misma en el servidor externo de contabilidad y el Prestige.	
Cuando haya completado este menú, pulse [ENTER] cuando aparezca la línea de mensaje “Press ENTER to confirm or ESC to cancel” para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla anterior.		

28.1.3 IEEE802.1x

El estándar IEEE802.1x muestra las métodos de seguridad tanto para la autenticación de las estaciones inalámbricas como para la gestión de las claves de encriptación.

Siga los siguientes pasos para habilitar la autenticación EAP en el Prestige.

Paso 1. Desde el menú principal, teclee 23 para mostrar el **Menu 23 – System Security**.

```
Menu 23 - System Security

    1. Change Password
    2. RADIUS Server

    4. IEEE802.1x
```

Figura 28-4 Menu 23 Seguridad del Sistema

Paso 2. Introduzca 4 para mostrar el **Menu 23.4 – System Security – IEEE802.1x**

```
                Menu 23.4 - System Security - IEEE802.1x

    Wireless Port Control= Authentication Required
    ReAuthentication Timer (in second)= 1800
    Idle Timeout (in second)= 3600


    Key Management Protocol= WPA
    Dynamic WEP Key Exchange= N/A
    PSK= N/A
    WPA Mixed Mode= Disable
    Data Privacy for Broadcast/Multicast packets= TKIP
    WPA Broadcast/Multicast Key Update Timer= 1800

    Authentication Databases= Local User Database Only


                Press ENTER to Confirm or ESC to Cancel:
```

Figura 28-5 Menu 23.4 Seguridad del Sistema : IEEE802.1x

La siguiente tabla describe los campos en este menú.

Tabla 28-2 Menu 23.4 Seguridad del Sistema : IEEE802.1x

CAMPO	DESCRIPCIÓN
Wireless Port Control	Presione [BARRA ESPACIADORA] y seleccione un modo de seguridad para el acceso de las estaciones de la LAN inalámbrica. Seleccione **No Authentication Required** para permitir a cualquier estación inalámbrica acceder a la red cableada sin necesidad de introducir nombres de usuario ni contraseña. Ésta es la configuración por defecto. Seleccione **Authentication Required** para forzar a las estaciones inalámbricas a introducir un nombre de usuario y contraseña antes de permitirle el acceso a la red cableada. Seleccione **No Access Allowed** para bloquear el acceso de todas las estaciones inalámbricas a la red cableada. Los siguientes campos no estarán disponibles cuando se seleccionen las opciones de **No Authentication Required** o **No Access Allowed**.
ReAuthentication Timer (en seg.)	Especifique cada cuanto tiempo ha de re-introducir un cliente su nombre de usuario y contraseña para permanecer conectado a la red cableada. Este campo estará activado únicamente cuando se seleccione **Authentication Required** en el campo **Wireless Port Control**. Introduzca un intervalo de tiempo entre 10 y 9999 (en segundos). El intervalo de tiempo por defecto es **1800** seg. (ó 30 minutos).
Idle Timeout (en	El Prestige automáticamente desconecta un cliente de la red cableada tras un periodo

segundos)	de inactividad. El cliente necesitará introducir el nombre de usuario y contraseña nuevamente antes de permitírsele el acceso a la red cableada. Este campo está activado únicamente cuando se seleccione **Authentication Required** en el campo **Wireless Port Control**. El intervalo de tiempo por defecto es de **3600** segundos (ó 1 hora).
Key Management Protocol	Presione la [BARRA ESPACIADORA] para seleccionar **802.1x, WPA** o **WPA-PSK** y pulse [INTRO].
Dynamic WEP Key Management	Este campo está activado sólo cuando se selecciona **Authentication Required** en el campo **Wireless Port Control**. También habrá que configurar el campo **Authentication Databases** como **RADIUS Only**. La base de datos local no puede ser utilizada. Seleccione **Disable** para permitir a las estaciones inalámbricas comunicarse con los puntos de acceso sin utilizar el Intercambio de Clave WEP Dinámica. Seleccione **64-bit WEP** ó **128-bit WEP** para habilitar la encriptación de datos. Hasta 32 estaciones pueden acceder al Prestige cuando se configura el Intercambio de Clave WEP Dinámica. Este campo no estará disponible cuando se configure el campo **Key Management Protocol** a **WPA** ó **WPA-PSK**.
PSK	Introduzca la clave entre 8 y 63 caracteres ASCII (incluyendo espacios y símbolos) cuando se seleccione **WPA-PSK** en el campo **Key Management Protocol**.
WPA Mixed Mode	Seleccione **Enable** para activar el modo mezclado WPA. De otra forma, seleccione **Disable** y configure el campo **Group Data Privacy**.
Data Privacy for Broadcast/Multicast packets	Este campo permite seleccionar **TKIP** (recomendado) o **WEP** para el tráfico broadcast y multicast si el **Key Management Protocol** está en **WPA** y el **WPA Mixed Mode** está deshabilitado. **WEP** será utilizado automáticamente si se tiene habilitado el **WPA Mixed Mode**. Todo el tráfico unicast es encriptado automáticamente con **TKIP** cuando **WPA** o **WPA-PSK** están seleccionados.
WPA Broadcast/Multicast Key Update Timer	El valor de este campo indica cada cuanto tiempo el punto de acceso (si está utilizando una clave de gestión **WPA-PSK**) o el servidor RADIUS (si se está utilizando **WPA**) envía un nuevo grupo de claves a todos los clientes. El proceso de refresco de claves para WPA es equivalente al cambiar automáticamente la clave WEP para un AP y todas las estaciones en una red WLAN básica. La configuración de este parámetro también está soportada para el modo WPA-PSK. El Prestige tiene por defecto un valor de **1800** segundos (30 minutos).
Authentication Databases	Las bases de datos de autenticación contienen la información de las estaciones inalámbricas. La base de datos local es la base de datos integrada en el Prestige. El RADIUS es un servidor externo. Utilice este campo para decidir que base de datos

	utilizará el Prestige en primer lugar para autenticar a las estaciones inalámbricas. Antes de especificar la prioridad, asegúrese que se han configurado las bases de datos correctamente. Cuando se configure el **Key Management Protocol** a **WPA**, la **Authentication Databases (Base de Datos de Autenticación)** deberá ser **RADIUS Only**. Sólo es posible utilizar la **Base de Datos Local (Local User Databases**) cuando se esté utilizando **802.1x**. Seleccione **Local User Database Only** para que el Prestige únicamente compruebe la base de datos interna del Prestige en busca del nombre de usuario y contraseña de una estación wireless. Seleccione **RADIUS Only** para que el Prestige únicamente compruebe la base de datos del servidor RADIUS especificado en busca del nombre de usuario y contraseña de una estación inalámbrica. Seleccione **Local first, then RADIUS** para que el Prestige chequee en primer lugar la base de datos del Prestige en busca del nombre de usuario y contraseña de una estación inalámbrica. Si el nombre de usuario no se encuentra, el Prestige comprobará este nombre de usuario en la base de datos del servidor RADIUS especificado. Seleccione **RADIUS first, then Local** para que el Prestige chequee en primer lugar la base de datos en el servidor RADIUS especificado en busca del nombre de usuario y contraseña de una estación wireless. Si el Prestige no puede contactar con el RADIUS, el Prestige pasará a buscar el nombre de usuario en la base de datos del Prestige. Cuando el nombre de usuario no se localiza o la contraseña no coincide en la base de datos del servidor RADIUS, el Prestige no comprobará la base de datos local y la autenticación fallará.
Cuando haya completado este menú, presione [INTRO] en la línea de mensaje “Press ENTER to confirm…” para guardar la configuración o pulse [ESC] para cancelar y volver a pantalla anterior.	

Una vez que se habilite la autenticación de usuario, será necesario especificar un servidor RADIUS externo o crear cuentas de usuario locales en el Prestige para la autenticación.

28.2 Creación de Cuentas de Usuario en el Prestige

Almacenando los perfiles de usuario localmente, el Prestige es capaz de autenticar a los usuarios inalámbricos sin necesidad de interactuar con un servidor RADIUS de red.

Siga los pasos indicados a continuación para configurar los perfiles de usuario en su Prestige.

Paso 1. Desde el menú principal, introducir 14 para mostrar el **Menu 14 –Dial-in User Setup**.

```
                    Menu 14 - Dial-in User Setup

   1. ________       9.  ________      17. ________      25. ________
   2. ________       10. ________      18. ________      26. ________
   3. ________       11. ________      19. ________      27. ________
   4. ________       12. ________      20. ________      28. ________
   5. ________       13. ________      21. ________      29. ________
   6. ________       14. ________      22. ________      30. ________
   7. ________       15. ________      23. ________      31. ________
   8. ________       16. ________      24. ________      32. ________

                    Enter Menu Selection Number:
```

Figura 28-6 Menu 14 Dial-in User Setup

Paso 2. Introduzca un número y presione [INTRO] para editar el perfil de usuario.

```
                 Menu 14.1 - Edit Dial-in User

                User Name= test
                Active= Yes
                Password= ********

                Press ENTER to Confirm or ESC to Cancel:
```

Figura 28-7 Menu 14.1 Edición de un Peril de Usuario

La siguiente tabla describe los campos de este menú.

Tabla 28-3 Menu 33-3 Menu 14.1 Edición de un Perfil de Usuario

CAMPO	DESCRIPCIÓN
User Name	Introduzca un nombre de usuario de hasta 31 caracteres alfanuméricos para este perfil de usuario. El caso es sensible a mayúsculas y minúsculas.
Active	Presione [BARRA ESPACIADORA] para seleccionar Yes y pulse [INTRO] para habilitar el perfil de usuario.
Password	Introduzca una contraseña de hasta 31 caracteres para este perfil.
Cuando haya completado este menú, presione [INTRO] en la línea de comando “Press ENTER to confirm…” para guardar la configuración o pulse [ESC] para cancelar y volver a la pantalla anterior.	

Capítulo 29
Información de Sistema y Diagnóstico

Este capítulo cubre la información y las herramientas de diagnóstico en los menús 24.1 a 24.4 del SMT.

Estas herramientas incluyen actualizaciones sobre el estado del sistema, estado de los puertos, capacidades de log y trazas y actualizaciones del software del sistema. Este capítulo describe como utilizar estas herramientas en detalle.

Introduzca 24 en el menú principal para abrir el **Menu 24 – System Maintenance**, como muestra en la siguiente figura.

```
                    Menu 24 - System Maintenance


                    1.  System Status
                    2.  System Information and Console Port Speed
                    3.  Log and Trace
                    4.  Diagnostic
                    5.  Backup Configuration
                    6.  Restore Configuration
                    7.  Upload Firmware
                    8.   Command Interpreter Mode
                    9.   Call Control
                    10. Time and Date Setting
                    11. Remote Management



                    Enter Menu Selection Number:
```

Figura 29-1 Menu 24 Mantenimiento del Sistema

29.1 Estado del Sistema

En la primera selección, System Status da información del estado y estadísticas de los puertos, como se muestra a continuación**¡Error! No se encuentra el origen de la referencia.**. El System Status es una herramienta que puede ser usada para monitorizar el Prestige. Específicamente, da información sobre el estado de la línea ADSL, número de paquetes enviados y recibidos.

Para llegar al System Status, teclee 24 para ir al **Menu 24 — System Maintenance.** Desde este menú, teclee 1**. System Status**. Hay dos comandos en el **Menu 24.1 — System Maintenance — Status**. Pulsando el 1 se resetean los contadores; pulsando [ESC] se vuelve a la pantalla anterior.

```
                    Menu 24.1 - System Maintenance - Status          04:35:40
                                                        Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s     Up Time
 1-1483  N/A              0           0           0       0       0     0:00:00
 2       N/A              0           0           0       0       0     0:00:00
 3       N/A              0           0           0       0       0     0:00:00
 4       N/A              0           0           0       0       0     0:00:00
 5       N/A              0           0           0       0       0     0:00:00
 6       N/A              0           0           0       0       0     0:00:00
 7       N/A              0           0           0       0       0     0:00:00
 8       N/A              0           0           0       0       0     0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                    WAN:
      Status:                 Tx Pkts: 593         Line Status: Down
      Collisions: 0           Rx Pkts: 0           Upstream Speed:     0 kbps
    CPU Load =    1.60%                            Downstream Speed:     0 kbps
                                  Press Command:
                     COMMANDS: 1-Reset Counters  ESC-Exit
```

Figura 29-2 Menu 24.1 Mantenimiento de Sistema : Estado

La siguiente tabla describe los campos presentes en el **Menu 24.1** — **System Maintenance** — **Status** que son campos de sólo lectura y nos facilitan información de diagnóstico.

Tabla 29-1 Menu 24.1 Mantenimiento de Sistema : Estado

CAMPO	DESCRIPCIÓN
Node-Lnk	Es el número de índice de nodo y el tipo de enlace. Los tipos de enlace son: PPP, ENET, 1483.
Status	Muestra el estado del nodo remoto.
TxPkts	El número de paquetes transmitidos al nodo remoto.
RxPkts	El número de paquetes recibidos del nodo remoto.
Errors	El número de paquetes erróneos en esta conexión.
Tx B/s	Muestra la tasa de transmisión en bytes por segundo.
Rx B/s	Muestra la tasa de recepción en bytes por segundo.
Up Time	Hora a la que este canal se ha conectado con el nodo remoto actual .
My WAN IP (from ISP)	La dirección IP del nodo remoto ISP.
Ethernet	Muestra las estadísticas de la LAN.
Status	Muestra el estado actual de la LAN.

Tx Pkts	El número de paquetes transmitidos a la LAN.
Rx Pkts	El número de paquetes recibidos de la LAN.
Collision	Número de colisiones.
WAN	Muestra las estadísticas de la WAN.
Line Status	Muestra el estado actual de la línea xDSL, que puede ser Up (Levantada) o Down (Caída).
Upstream Speed	Muestra la tasa de transferencia del canal de subida en Kbps.
Downstream Speed	Muestra la tasa de transferencia del canal de bajada en Kbps.
CPU Load	Especifica el porcentaje de utilización de la CPU.

29.2 Información del Sistema

Para obtener la información del sistema:

Paso 1. Teclee 24 para mostar el **Menu 24 – System Maintenance**.

Paso 2. Teclee 2 para mostrar el **Menu 24.2 – System Information and Console Port Speed**.

Paso 3. Desde este menú tiene dos opciones como se muestra en la siguiente figura:

```
        Menu 24.2 - System Information and Console Port Speed
              1. System Information
              2. Console Port Speed



                     Please enter selection:
```

Figura 29-3 Menu 24.2 Información de Sistema y Velocidad del Puerto de Consola

El Prestige tiene un puerto de consola interno únicamente para personal de soporta. No abra el Prestige o perderá la garantía del mismo.

29.2.1 Información del Sistema

Introduzca 1 en el menú 24.2 para mostrar la pantalla que se indica a continuación.

```
Menu 24.2.1 - System Maintenance - Information

   Name:
   Routing: IP
   ZyNOS F/W Version: V3.40(PE.0)b1 | 12/18/2003
   ADSL Chipset Vendor: TI AR7 01.01.00.00
   Standard: NORMAL

   LAN
     Ethernet Address: 00:a0:c5:6a:df:f4
     IP Address: 192.168.1.1
     IP Mask: 255.255.255.0
     DHCP: Server


         Press ESC or RETURN to Exit:
```

Figura 29-4 Menu 24.2.1 Mantenimiento del Sistema : Información

La siguiente tabla describe los campos de este menú.

Tabla 29-2 Menu 24.2.1 Mantenimiento del Sistema : Información

CAMPO	DESCRIPCIÓN
Name	Muestra el nomre del sistema del Prestige. Esta información se puede cambiar en el **Menu 1 – General Setup**.
Routing	Se refiere al protocolo de enrutamiento utilizado.
ZyNOS F/W Version	Se refiere al ZyNOS (ZyXEL Network Operating System), versión firmware del sistema. ZyNOS es un marca registrada de ZyXEL Communications Corporation.
ADSL Chipset Vendor	Muestra el nombre del vendedor del chipset ADSL y de la versión DSL.
Standard	Se refiere al protocolo operacional que el Prestige y el DSLAM (Digital Subscriber Line Access Multiplexer) están usando.
LAN	
Ethernet Address	Se refiere a la Ethernet MAC (Media Access Control) del Prestige.
IP Address	Es la dirección IP del Prestige en notación decimal.
IP Mask	Muestra la máscara de subred del Prestige.
DHCP	Este campo muestra la configuración DHCP setting (None, Relay or Server) del Prestige.

29.2.2 Velocidad del Puerto de Consola

Se pueden configurar diferentes velocidades del puerto consola a través del Menu 24.2.2 – Sistem Maintenance – Console Port Speed. Su Prestige soporta 9600 (por defecto), 19200, 38400, 57600 y 115200 bps. Presione [BARRA ESPACIADORA] y a continuación [INTRO] para seleccionar la velocidad deseada en el menú 24.2.2, como se muestra en la siguiente figura.

```
        Menu 24.2.2 - System Maintenance - Change Console Port Speed

                        Console Port Speed: 9600

                   Press ENTER to Confirm or ESC to Cancel:
```

Figura 29-5 Menu 24.2.2 Mantenimiento del Sistema : Cambiar la Velocidad de la Consola

Una vez modificada la velocidad del puerto de consola del Prestige, será necesario ajustar la velocidad en el software de comunicaciones utilizado para comunicarse con el Prestige.

29.3 Log y Traza

Existen dos posibilidades de registro en el Prestige. El primero es el registro de errores y la grabación de la traza que se almacena localmente. El segundo es la facilidad de syslog de UNIX para el registro de mensajes.

29.3.1 Visualización del Registro de Error

El primer sitio donde se deben buscar pistas cuando algo va mal es en el log de errores. Siga el procedimiento para visualizar el registro de errores local:

Paso 1. Introduzca 24 en el menú principal para mostrar el **Menu 24 – System Maintenance**.

Paso 2. Desde el menú 24, teclee 3 para mostrar el **Menu 24.3 – System Maintenance – Log and Trace**.

```
            Menu 24.3 - System Maintenance - Log and Trace


               1. View Error Log
               2. UNIX Syslog




                     Please enter selection
```

Figura 29-6 Menu 24.3 Mantenimiento del Sitema : Log y Traza

Paso 3. Teclee 1 desde el Menu 24.3 – System Maintenance – Log and Trace para mostrar el log de errores del sistema.

Cuando el Prestige termina de mostrar el log de errores, nos mostrará la opción para borrarlo. Ejemplos de errores típicos y algunos mensajes de información se presentan en la siguiente figura.

```
  59 Thu Jan 01 00:00:03 1970 PP0f  INFO  LAN promiscuous mode <0>
  60 Thu Jan 01 00:00:03 1970 PP00 -WARN  SNMP TRAP 0: cold start
  61 Thu Jan 01 00:00:03 1970 PP00  INFO  main: init completed
  62 Thu Jan 01 00:00:19 1970 PP00  INFO  SMT Session Begin
  63 Thu Jan 01 00:00:24 1970 PP0a  WARN  MPOA Link Down
Clear Error Log (y/n):
```

Figura 29-7 Muestra de Error y Mensajes de Información

29.3.2 Syslog y Contabilidad

El Prestige utiliza la facilidad UNIX Syslog para registro de CDR (Call Detail Record – Almacenamiento de Detalles de Llamada) y mensajes del sistema en un servidor syslog. El syslog y la contabilidad pueden ser configurados en el Menu 24.3.2 – System Maintenance – UNIX Syslog, como se indica.

```
                Menu 24.3.2 - System Maintenance - UNIX Syslog

                      UNIX Syslog:
                      Active= No
                      Syslog IP Address= ?
                      Log Facility= Local 1



                   Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figura 29-8 Menu 24.3.2 Mantenimiento del Sistema : Syslog y Contabilidad

Será necesario configurar los parámetros del UNIX syslog descritos en la siguiente tabla para activar el syslog, después seleccione lo que desea registrar.

Tabla 29-3 Menu 24.3.2 Mantenimiento del Sistema : Syslog y Contabilidad

PARÁMETRO	DESCRIPCIÓN
UNIX Syslog:	
Active	Use la barra espaciadora [SPACE BAR] y luego [ENTER] para activar o desactivar el syslog.
Syslog IP Address	Introduzca la dirección IP del servidor syslog.
Log Facility	Use la barra espaciadora [SPACE BAR] y luego [ENTER] para seleccionar una de las siete opciones locales diferentes. Permite registrar los mensajes en siete ficheros de servidor diferentes. Vea su manual de UNÍS.

A continuación se muestran ejemplos de cuatro tipos de mensajes syslog enviados por el Prestige:

1 – CDR
SdcmdSyslogSend (SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)
C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxx (= connected speed) xxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002 Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002 Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
2 - Packet Triggered
SdcmdSyslogSend (SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768

696a6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=450000282401400 01f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
3 – Filter Log
SdcmdSyslogSend (SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m), drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol (“TCP”, ”UDP”, ”ICMP”)
spo: Source port
dpo: Destination port
Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP spo=0208 dpo=0208]} S03>R01mF Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035]} S03>R01mF
4 – PPP Log
SdcmdSyslogSend (SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP
Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing

29.4 Diagnóstico

La facilidad de diagnóstico permite comprobar diferentes aspectos de su Prestige para determiner si está funcionando adecuadamente. El Menú 24.4 permite seleccionar entre varios tipos de tests de diagnóstico para evaluar el sistema, como se muestra en la siguiente figura.

Siga el siguiente procedimiento para pasar al diagnóstico:

Paso 1. Desde el menú principal, introduzca 24 para abrir el **Menu 24 – System Maintenance**.

Paso 2. Desde este menú, teclee 4. Se abrirá el diagnóstico del **Menu 24.4 – System Maintenance – Diagnostic**.

```
                  Menu 24.4 - System Maintenance - Diagnostic

xDSL                                        System
1.  Reset xDSL                              21. Reboot System
                                            22. Command Mode

TCP/IP
12. Ping Host

                          Enter Menu Selection Number:
                    Host IP Address= N/A
```

Figura 29-9 Menu 24.4 Mantenimiento del Sistema : Diagnóstico

La siguiente tabla describe los tests de diagnóstico disponibles en el menú 24.4 para las conexiones.

Tabla 29-4 Menu 24.4 Mantenimiento del Sistema : Diagnóstico

CAMPO	DESCRIPCIÓN
Reset xDSL	Reinicia el enlace xDSL.
Ping Host	Hace un **Ping** al host para ver si el enlace y el protocolo TCP/IP funcionan en ambos sistemas.
Reboot System	Reinicia el Prestige.
Command Mode	Pasar al modo comando para chequear el estado del Prestige utilizando comandos específicos.
Host IP Address	Si ha puest 12 para hacer Ping al Host, introduzca aquí la dirección del sistema al que quiere realizar el ping.

Capítulo 30
Mantenimiento de Firmware y Fichero de Configuración

Este capítulo indica como hacer un backup y una carga del fichero de configuración así como la actualización de nuevos ficheros de firmware y de configuración.

30.1 Convenciones sobre Nombres de Fichero

El fichero de configuración (habitualmente llamadao fichero rom o rom-0) contiene las configuraciones por defecto de fábrica en los menús tales como contraseñas, configuración DHCP, configuración TCP/IP, etc. El archivo llega de ZyXEL con extensión “rom”. Una vez que se haya personalizado la configuración del Prestige, puede ser grabado con otro nombre de fichero a su elección.

ZyNOS (ZyXEL Network Operating System, algunas veces referido al fichero “ras”) es el firmware de sistema y tiene una extensión de fichero “bin”. Con muchos clientes FTP and TFTP, el trato de los ficheros es muy similar a como se muestra a continuación.

Utilice sólo el firmware específico para su modelo Prestige. Consulte la etiqueta en la parte de debajo de su Prestige.

```
ftp> put firmware.bin ras
```

Este es un ejemplo de sesión FTP mostrando la transferencia del archivo "firmware.bin" al Prestige.

```
ftp> get rom-0 config.cfg
```

Este es un ejemplo de sesión FTP guardando la configuración actual en el fichero “config.cfg”.

Si su cliente (T)FTP no permite tener archivos de destino con diferente nombre del archivo fuente, necesitará renombrarlos, ya que el Prestige solamente reconoce “rom-0” y “ras”. Asegúrese de que mantiene copias inalteradas de ambos ficheros para su posterior uso.

La siguiente tabla es un resumen. Por favor, tenga en cuenta que el nombre de archivo interno se refiere al nombre de archivo en el Prestige y el nombre de archivo externo se refiere al nombre de fichero no en el Prestige, esto es, en su ordenador, red local o DTP y por tanto, el nombre (pero no la extensión) pueden variar. Después de actualizar el firmware, vea el campo **ZyNOS F/W Version** en el **Menu 24.2.1 – System Maintenance – Information** para confirmar que ha actualizado a la versión correcta de firmware. El

comando AT es el comando que se introduce después de pulsar “y” cuando le aparezca un mensaje en el menú SMT para entrar en modo debug.

Tabla 30-1 Convenciones sobre Nombres de Fichero

TIPO DE FICHERO	NOMBRE INTERNO	NOMBRE EXTERNO	DESCRIPCIÓN
Configuration File	Rom-0	Es el fichero de configuración del Prestige. Actualizando el fichero rom-0 se sustituye el sistema de ficheros ROM entero, incluyendo las configuraciones del Prestige, datos relacionados con el sistema (incluyendo la contraseña por defecto), el registro de error y el registro de traza.	*.rom
Firmware	Ras	Es el nombre genérico del firmware de ZyNOS en el Prestige.	*.bin

30.2 Backup de Configuración

La opción 5 del **Menu 24 – System Maintenance** permite hacer backup de la configuración actual del Prestige en su PC. Es muy recomendable hacerlo una vez que el Prestige funcione correctamente. FTP es el método preferido para realizar el backup de la configuración debido a que es el más rápido. También puede llevar a cabo el backup y la recuperación usando el menú 24 a través del puerto de consola. Cualquier programa de comunicaciones serie debería funcionar bien; sin embargo, debe utilizar el protocolo Xmodem para llevar a cabo la descarga y carga del fichero, sin necesidad de renombrar los ficheros.

Por favor, tenga en cuenta que cuando hablamos de descarga nos referimos a transferencia del Prestige al ordenador, mientras que carga se refiere a la transferencia entre ordenador y Prestige.

30.2.1 Backup de la Configuración

Siga las instrucciones que se muestran en la siguiente pantalla.

```
                Menu 24.5 - System Maintenance - Backup Configuration

 To transfer the configuration file to your workstation, follow the procedure
 below:

 1. Launch the FTP client on your workstation.
 2. Type "open" and the IP address of your Prestige. Then type "root" and
    SMT password as requested.
 3. Locate the 'rom-0' file.
 4. Type 'get rom-0' to back up the current Prestige configuration to
    your workstation.

 For details on FTP commands, please consult the documentation of your FTP
 client program. For details on backup using TFTP (note that you must remain
 in this menu to back up using TFTP), please see your Prestige manual.


                              Press ENTER to Exit:
```

Figura 30-1 Telnet en el Menu 24.5

30.2.2 Utilización del comando FTP desde la Línea de Comando

Paso 3. Lance el cliente FTP en su ordenador.

Paso 4. Teclee “open”, seguido de un espacio y la dirección IP de su Prestige.

Paso 5. Presione [INTRO] cuando se le pida el nombre de usuario.

Paso 6. Introduzca la contraseña cuando se le pida (por defecto es 1234).

Paso 7. Teclee “bin” para activar el modo de transferencia binario.

Paso 8. Utilice “get” para transferir ficheros desde el Prestige al ordenador, por ejemplo, “get rom-0 config.rom” transfiere el fichero de configuration del Prestige al ordenador y lo renombra como “config.rom”. Vea las primeras secciones de este capítulo para más información sobre las convenciones del nombre de los ficheros.

Paso 9. Teclee “quit” para salir del prompt ftp.

30.2.3 Ejemplo de Comandos FTP desde la Línea de Comando

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figura 30-2 Ejemplo de Sesión

30.2.4 Clientes FTP basados en GUI (Interfaces Gráficos)

La siguiente tabla describe algunos de los comandos que podrá ver en los clientes FTP basados en interfaces gráficos.

Tabla 30-2 Comandos Generales para Clientes FTP con Interfaces Gráficos

COMANDO	DESCRIPCIÓN
Host Address	Introduzca la dirección del host.
Login Type	Anonymous: Se produce cuando una identidad de usuario y contraseña es suministrada automáticamente por el servidor para un acceso anónimo. Este tipo de accesos funcionará solamente si su ISP o administrador de servicios tiene esta opción habiltada Normal: El servidor requiere un par identidad de usuario-contraseña único.
Transfer Type	Transfiere archivos en ASCII (formato de texto legilble) o en modo binario.
Initial Remote Directory	Especifique el directorio remoto por defecto (path).
Initial Local Directory	Especifique el directorio local por defecto (path).

30.2.5 Limitaciones de la Gestión TFTP y FTP sobre la WAN

El acceso TFTP, FTP y Telnet sobre la WAN no funcionarán adecuadamente cuando:

1. Se ha deshabilitado el servicio Telnet en el menú 24.11.
2. Se ha aplicado un filtro en el menú 3.1 (LAN) o en el menú 11.5 (WAN) para bloquear el servicio Telnet.
3. La dirección IP en el campo **Secured Client IP** del menú 24.11 no coincide con la dirección IP del cliente. Si no coincide, el Prestige desconectará la sesión Telnet de forma inmediata.
4. Existe una sesión de consola SMT ejecutándose.

30.2.6 Backup de la Configuración utilizando TFTP

El Prestige soporta la carga/descarga de los ficheros de firmware y de configuración utilizando TFTP (Trivial File Transfer Protocol) sobre LAN. Aunque TFTP puede operar también sobre WAN, es algo que no se recomienda.

Para usar TFTP, el ordenador debe contar tanto con un cliente telnet como TFTP. Para hacer un backup de la configuración, siga el siguiente procedimiento.

Paso 1. Utilice telnet desde su ordenador para conectar con el Prestige y registrarse. Dado que el TFTP no tiene ningún tipo de seguridad, el Prestige almacenará la dirección IP del cliente telnet y aceptará las peticiones TFTP sólo desde esta dirección.

Paso 2. Coloque el SMT del Prestige en modo comando accediendo al submenú 8 dentro del **Menu 24 – System Maintenance**.

Paso 3. Teclee el comando “sys stdio 0” para deshabilitar el temporizador de inactividad del SMT, de manera que la transferencia TFTP no será interrumpida. Introduzca el comando “sys stdio 5” para restaurar los 5 minutos del temporizador del SMT (por defecto) cuando la transferencia del fichero se haya completado.

Paso 4. Lance el cliente TFTP en su ordenador y conecte con el Prestige. Configure la transferencia en modo binario antes de transferir los datos.

Paso 5. Utilice el cliente TFTP (vea el ejemplo siguiente) para transferir ficheros entre el Prestige y el ordenador. El nombre del fichero para el fichero de configuración es “rom-0”.

Tenga en cuenta que la conexión telnet debe estar activa y el SMT en modo CI antes y durante la transferencia TFTP. Para más detalles sobre los comandos TFTP (vea el siguiente ejemplo), por favor consulte la documentación su programa de cliente TFTP. En UNIX, use “get” para transferir desde el Prestige al ordenador y “binary” para poner el modo de transferencia binario.

30.2.7 Ejemplo Comandos TFTP

A continuación se muestra un ejemplo con los comandos TFTP:

```
tftp [-i] host get rom-0 config.rom
```

donde “i” especifica el modo de transferencia binario (use este modo para transferir ficheros binarios), “host” es la dirección IP del Prestige, “get” transfiere el fichero origen del Prestige (rom-0, nombre del fichero de configuración en el Prestige) al fichero destino en el ordenador y renómbrelo como config.rom.

30.2.8 Clientes TFTP basados en GUI

La siguiente tabla describe algunos de los campos que podrá encontrar con clientes TFTP basados en interfaces gráficos.

Tabla 30-3 Comandos Generales con clientes TFTP con Interfaz Gráfica

COMANDO	DESCRIPCIÓN
Host	Introduzca la dirección IP del Prestige. 192.168.1.1 es la dirección IP por defecto del Prestige de fábrica.
Send/Fetch	Use “Send” para cargar el fichero del Prestige y “Fetch” para hacer un backup del fichero en su PC.
Local File	Introduzca el path y el nombre del fichero de firmware (extension *.bin) o el fichero de configuración (extensión *.rom) en su PC.
Remote File	Es el nombre del fichero del Prestige. El nombre del fichero de firmware es “ras” y del fichero de configuración es “rom-0”.
Binary	Transferir en fichero en modo binario.
Abort	Detiene la transferencia del fichero.

Consulte la sección 30.2.5 para ver información relativa a configuraciones que no permiten la configuración TFTP y FTP a través de WAN.

30.3 Restauración de la Configuración

Esta sección muestra cómo restaurar una configuración que previamente ha sido guardada. Tenga en cuenta que esta función borrará la configuración actual; por favor, no intente restablecerla a no ser que tenga una configuración de backup correcta almacenada en disco.

FTP es el método preferido para restablecer la configuración actual del Prestige, debido a que es el método más rápido. Tenga en cuenta que debe esperar a que el sistema reinicie automáticamente después de que haya completado la transferencia del fichero.

ATENCIÓN!
NO INTERRUMPA EL PROCESO DE TRANSFERENCIA DEL FICHERO YA QUE ESTO PUEDE CAUSAR UN DAÑO PERMANENTE AL PRESTIGE.

30.3.1 Restauración utilizando FTP

Para detalles sobre la restauración utilizando (T)FTP, por favor, consulte secciones previas sobre la carga de ficheros a través de FTP y TFTP.

```
                 Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and
   SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-0 is the
   remote file name on the Prestige. This restores the configuration to
   your Prestige.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.


                              Press ENTER to Exit:
```

Figura 30-3 Telnet en el Menu 24.6

Paso 1. Lance el cliente FTP en su ordenador.

Paso 2. Teclee “open”, seguido de un espacio y la dirección IP de su Prestige.

Paso 3. Pulse [INTRO] cuando se le pida el nombre de usuario.

Paso 4. Introduzca la contraseña cuando se le pida (por defecto 1234).

Paso 5. Teclee “bin” para colocar la transferencia en modo binario.

Paso 6. Localice el fichero “rom” (en su ordenador) que quiere restaurar en el Prestige.

Paso 7. Utilice “put” para transferir el fichero del ordenador al Prestige, for ejemplo, “put config.rom rom-0” transfiere el fichero de configuración “config.rom” del ordenador al Prestige. Consulte en secciones previas las convenciones sobre el nombre de los ficheros.

Paso 8. Teclee “quit” para salir del símbolo del ftp. El Prestige se reiniciará automáticamente tras un proceso de restauración satisfactorio.

30.3.2 Ejemplo de Restauración utilizando una sesión FTP

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Figura 30-4 Ejemplo de Restauración utilizando una sesión FTP

Consulte la sección 30.2.5 para ver configuraciones que limitan el TFTP y el FTP a través de WAN.

30.4 Carga de Ficheros de Firmware y de Configuración

Este apartado muestra cómo cargar el firmware y los archivos de configuración. Puede cargar los archivos de configuración siguiendo el procedimiento indicado en la sección anterior o las instrucciones del **Menu 24.7.2 – System Maintenance – Upload System Configuration File.**

AVISO!

NO INTERRUMPA EL PROCESO DE TRANSFERENCIA O PODRÁ OCASIONAR DAÑOS PERMANENTES EN SU PRESTIGE.

30.4.1 Carga del Fichero de Firmware

FTP es el método preferido para cargar el firmware y la configuración. Para utilizar este método, su ordenador debe tener un cliente FTP.

Cuando se conecte al Prestige vía telnet, verá las siguientes pantallas para carga del firmware y del fichero de configuración usando FTP.

```
                  Menu 24.7.1 - System Maintenance - Upload System Firmware

     To upload the system firmware, follow the procedure below:

       1. Launch the FTP client on your workstation.
       2. Type "open" and the IP address of your system. Then type "root" and
          SMT password as requested.
       3. Type "put firmware filename ras" where "firmwarefilename" is the name
          of your firmware upgrade file on your workstation and "ras" is the
          remote file name on the system.
       4. The system reboots automatically after a successful firmware upload.


     For details on FTP commands, please consult the documentation of your FTP
     client program. For details on uploading system firmware using TFTP (note
     that you must remain on this menu to upload system firmware using TFTP),
     please see your manual.

                                   Press ENTER to Exit:
```

Figura 30-5 Telnet en el Menu 24.7.1 Carga Firmware del Sistema

30.4.2 Carga del Fichero de Configuración

Verá la siguiente pantalla cuando haga telnet en el menú 24.7.2.

```
             Menu 24.7.2 - System Maintenance - Upload System Configuration File

    To upload the system configuration file, follow the procedure below:

      1. Launch the FTP client on your workstation.
      2. Type "open" and the IP address of your system. Then type "root" and
         SMT password as requested.
      3. Type "put configuration filename rom-0" where "configurationfilename"
         is the name of your system configuration file on your workstation, which
         will be transferred to the "rom-0" file on the system.
      4. The system reboots automatically after the upload system configuration
         file process is complete.

    For details on FTP commands, please consult the documentation of your FTP
    client program. For details on uploading system firmware using TFTP (note
    that you must remain on this menu to upload system firmware using TFTP),
    please see your manual.

                                  Press ENTER to Exit:
```

Figura 30-6 Telnet en el Menu 24.7.2 Mantenimiento del Sistema

Para cargar el fichero de firmware y de configuración, siga los siguientes ejemplos.

30.4.3 Actualización de ficheros a través de FTP desde la ventana de DOS

Paso 1. Lance el cliente FTP en su ordenador.

Paso 2. Teclee "open", seguido de un espacio y la dirección IP del Prestige.

Paso 3. Pulse [INTRO] cuando se le pregunte por el nombre de usuario.

Paso 4. Introduzca la contraseña cuando se le pida (por defecto es 1234).

Paso 5. Teclee "bin" para configurar el modo de transferencia binario.

Paso 6. Utilice "put" para transferir ficheros desde el ordenador al Prestige, por ejemplo, "put firmware.bin ras" transfiere el firmware desde el ordenador (firmware.bin) al Prestige y lo renombra como "ras". De forma similar, "put config.rom rom-0" transfiere el fichero de configuración del ordenador (config.rom) al Prestige y lo renombra como "rom-0". Asímismo "get rom-0 config.rom" transfiere el fichero de configuración del Prestige al ordenador y lo renombra como "config.rom". Vea secciones previas sobre convenciones sobre el nombre de los ficheros.

Paso 7. Introduzca "quit" para salir del símbolo ftp.

El Prestige se reinicia automáticamente tras una actualización de fichero satisfactoria.

30.4.4 Ejemplo de Carga del Fichero de Firmware con una sesión FTP

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figura 30-7 Ejemplo de Carga del Fichero de Firmware mediante FTP

Se pueden encontrar más comandos en secciones previas de este capítulo.

Consulte la sección 30.2.5 para ver algunas configuraciones en la que se encuentra deshabilitado el acceso TFTP y FTP sobre la WAN.

30.4.5 Carga de Fichero mediante TFTP

El Prestige también soporta la carga de ficheros de firmware utilizando TFTP sobre LAN. Aunque TFTP también podría operar sobre la WAN, no se recomienda.

Para usar TFTP, el ordenador deberá disponer tamto de un cliente telnet como TFTP. Para transferir el fichero de firmware y de configuración, siga el procedimiento que se indica.

Paso 8. Utilice telnet desde el ordenador para conectar con el Prestige y registrarse. Como TFTP no realiza ninguna comprobación de seguridad, el Prestige almacena la dirección IP del cliente telnet y acepta únicamente peticiones TFTP desde esta dirección.

Paso 9. Coloque el SMT en el interfaz de comandos tecleando 8 en el **Menu 24 – System Maintenance**.

Paso 10. Introduzca el comando “sys stdio 0” para deshabilitar el temporizador de inactividad, de manera que la transferencia TFTP no se interrumpa. Introduzca “sys stdio 5” para restaurar los cinco minutos del temporizador (por defecto) cuando se haya completado la transferencia del fichero.

Paso 11. Lance el cliente TFTP en el ordenador y conecte con el Prestige. Coloque el modo de transferencia en binario antes de comenzar la misma.

Paso 12. Utilice el cliente TFTP (ver el ejemplo siguiente) para transferir ficheros entre el Prestige y el ordenador. El nombre del fichero de firmware es “ras”.

Tenga en cuenta que la conexión telnet debe estar activa y el Prestige en modo CI antes y durante la transferencia TFTP. Para más detalles sobre comandos TFTP (vea el siguiente ejemplo), por favor, consulte la documentación del programa cliente TFTP que esté utilizando. En UNIX, use “get” para transferir del Prestige al ordenador, “put” del ordenador al Prestige, y “binary” para establecer como binario el modo de transferencia.

30.4.6 Ejemplo de Comandos para Carga a través del TFTP

El siguiente ejemplo es un comando TFTP:

```
tftp [-i] host put firmware.bin ras
```

donde “i” especifica el modo de transferencia binario (use este mode para transferir ficheros binarios), “host” es la dirección IP del Prestige y “put” transfiere el fichero origen del ordenador (firmware.bin – nombre del firmware en el ordenador) al fichero destino en el host remoto (ras – nombre del firmware en el Prestige).

Los comandos que puede ver en los clientes TFTP basados en GUI han sido listados previamente en este capítulo.

Capítulo 31
Mantenimiento del Sistema

Este capítulo muestra los menús 24.8 al 24.10 del SMT.

31.1 Modo Intérprete de Comandos

El Intérprete de Comandos (CI) es una parte del firmware del sistema principal. El CI proporciona muchas de las funcionalidades del SMT, al tiempo que permite configurar parámetros de bajo nivel y utilizar funciones de diagnóstico. Acceda al CI desde el SMT a través del menú 24.8. Vea el disco que se incluye con el Prestige o la web de zyxel.com para obtener más información sobre los comandos del CI. Pulse 8 en el **Menu 24 — System Maintenance**. Puede encontrar una lista de comandos válidos tecleando `help` o `?` en la línea de comandos. Introduzca "exit" para volver al menú SMT principal cuando haya terminado.

```
                Menu 24 - System Maintenance

               1.  System Status
               2.  System Information and Console Port Speed
               3.  Log and Trace
               4.  Diagnostic
               5.  Backup Configuration
               6.  Restore Configuration
               7.  Upload Firmware
               8.  Command Interpreter Mode
               9.  Call Control
               10. Time and Date Setting
               11. Remote Management


                Enter Menu Selection Number:
```

Figura 31-1 Modo Comando en Menu 24

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            ether           wan
wlan            ip              ipsec           bridge
lan             radius          8021x
ras>
```

Figura 31-2 Comandos Válidos

31.2 Soporte de Control de Llamadas

Soporte de Control de Llamadas sólo es aplicable cuando la **Encapsulation** está puesta a **PPPoE** en el menú 4 o menú 11.1.

La función de gestión de acceso le permite establecer un límite del tiempo total de conexión al exterior del Prestige. Cuando el total de llamadas salientes excede el límite, la conexión actual se desconecta y se bloquearán todos las llamadas salientes posteriores.

Para acceder al menú de control de llamadas, seleccione la opción 9 en el menú 24 para ir al **Menu 24.9 — System Maintenance — Call Control**, como muestra la siguiente tabla.

```
                 Menu 24.9 - System Maintenance - Call Control

                    1.  Budget Management



                         Enter Menu Selection Number:
```

Figura 31-3 Menu 24.9 Mantenimiento de Sistema : Control de Llamada

31.2.1 Gestión de acceso

El menú 24.9.1 muestra las estadísticas del control de acceso para llamadas salientes. Introduzca 1 en el **Menu 24.9 — System Maintenance — Call Control** para que aparezca el siguiente menú.

```
                Menu 24.9.1 - System Maintenance - Budget Management

  Remote Node        Connection Time/Total Budget      Elapsed Time/Total Period
 1.MyIsp                     No Budget                          No Budget
 2.--------                     ---                                ---
 3.--------                     ---                                ---
 4.--------                     ---                                ---
 5.--------                     ---                                ---
 6.--------                     ---                                ---
 7.--------                     ---                                ---
 8.--------                     ---                                ---

                       Reset Node (0 to update screen):
```

Figura 31-4 Menu 24.9.1 Mantenimiento de Sistema : Gestión de Acceso

El tiempo total de acceso (total budget) es el límite del tiempo acumulado para conexiones externas a un nodo remoto. Cuando se alcance el límite, la llamada será cortada y las posteriores conexiones salientes hacia el nodo remoto serán bloqueadas. Después de cada periodo, el tiempo total de acceso se resetea. Por defecto, el tiempo total es 0 minutes y el periodo es 0 horas, lo que significa que no hay control de acceso. Se puede resetear el tiempo de conexión acumulado en este menú tecleando el índice de un nodo remoto. Pulse 0 actualizar la pantalla. El tiempo total y el periodo de reset se pueden configurar en el menú 11.1 para el nodo remoto cundo está seleccionada la encapsulación PPPoE.

Tabla 31-1 Menu 24.9.1 Mantenimiento del Sitema : Gestión de Acceso

CAMPO	DESCRIPCIÓN	EJEMPLO
Remote Node	Introduzca el número de índice del nodo remoto que quiere resetear (solo uno en este caso)	1
Connection Time/Total Budget	Es el tiempo total de conexión que ha transcurrido (del asignado que se ha establecido en el menú 11.1).	5/10 significa que 5 minutos de un total asignado de 10 minutos han pasado.
Elapsed Time/Total Period	El periodo es el ciclo de tiempo en horas que pasa entre reseteos del tiempo asignado (vea el menú 11.1.). El tiempo transcurrido es el tiempo agotado dentro de este periodo.	0.5/1 significa que 30 minutos del periodo de 1 hora ha transcurrido.
Pulse “0” para actualizar la pantalla o pulse [ESC] para volver a la pantalla anterior.		

31.3 Configuración de Fecha y Hora

El Prestige guarda la información de hora y fecha. También hay un mecanismo software para fijar la hora manualmente o conseguir la hora y fecha actual de un servidor externo cuando encienda su Prestige. El menú 24.10 le permite actualizar las configuraciones de hora y fecha del Prestige. La hora real se guarda en los logs de error del Prestige.

Seleccione 10 en el menú principal para abrir el **Menu 24 — System Maintenance**.

```
                Menu 24 - System Maintenance

                1.  System Status
                2.  System Information
                3.  Log and Trace
                4.  Diagnostic
                5.  Backup Configuration
                6.  Restore Configuration
                7.  Upload Firmware
                8.  Command Interpreter Mode
                9.  Call Control
                10. Time and Date Setting
                11. Remote Management

                Enter Menu Selection Number:
```

Figura 31-5 Menu 24 Mantenimiento del Sistema

Luego pulse 10 para ir al **Menu 24.10 — System Maintenance — Time and Date Setting** para actualizar la configuración de hora y fecha como se ve en la pantalla.

```
          Menu 24.10 - System Maintenance - Time and Date Setting


     Use Time Server when Bootup= None
     Time Server Address= N/A

     Current Time:                          00 : 00 : 00
     New Time (hh:mm:ss):                   11 : 23 : 16

     Current Date:                          2000 - 01 - 01
     New Date (yyyy-mm-dd):                 2001 - 03 - 01

     Time Zone= GMT

     Daylight Saving= No
     Start Date (mm-dd):                        01 - 00
     End Date (mm_dd):                          01 - 00

               Press ENTER to Confirm or ESC to Cancel:
```

Figura 31-6 Menu 24.10 Mantenimiento del Sistema : Configuración de Fecha y Hora

Tabla 31-2 Menu 24.10 Mantenimiento del Sistema : Configuración Fecha y Hora

CAMPO	DESCRIPCIÓN
Use Time Server when Bootup	Introduzca el protocolo de servidor de tiempo que su servidor de tiempo envía cuando se enciende el Prestige. No todos los servidores de tiempo soportan todos los protocolos, así que puede tener que validar con su ISP/administrador de red o use prueba y error para encontrar un protocolo que funcione. Las principales diferencias entre ellos son el formato. El formato de **Daytime (RFC 867)** es día/mes/año/huso horario del servidor.
	El formato de **Time (RFC-868)** muestra un entero de 4 bytes que da el número total segundos desde 1970/1/1 a las 0:0:0. **NTP (RFC-1305)** es similar a **Time (RFC-868)**. **None**. Por defecto, introduzca la hora manualmente.
Time Server Address	Introduzca la dirección IP o el nombre de dominio del servidor de hora. Compruebe con ISP/administrador de red si no está seguro de esa información.
Current Time New Time	Este campo muestra la hora actualizada cuando vuelve a entrar a este menú. Introduzca la nueva hora en formato hora, minuto y segundo.
Current Date New Date	Este campo muestra una fecha actualizada solamente cuando accede a este menú. Introduzca la nueva fecha en formato año, mes y día.
Time Zone	Presione la barra espaciadora [SPACE BAR] y luego [ENTER] para establecer diferencia entre su huso horario y la hora del meridiano Greenwich (GMT).
Daylight Saving	Si usa ajuste horario de verano automático, elija **Yes**.
Start Date	Si usa ajuste horario de verano automático, introduzca el mes y día que debe iniciar.
End Date	Si usa ajuste horario de verano automático, introduzca el mes y día que debe finalizar.
Una vez que haya rellenado este menú, pulse [ENTER] cuando aparezca el mensaje "Press ENTER to Confirm or ESC to Cancel" para guardar su configuración, o pulse [ESC] para cancelar.	

31.3.1 Configuración de la Hora

El Prestige configura la hora en tres situaciones:

i. Al dejar el menú 24.10 tras hacer los cambios.

ii. Cuando el Prestige se inicia, si existe un servidor de tiempo configurado en el menú 24.10.

iii. En intervalos de 24 horas después del encendido.

Capítulo 32
Gestión Remota

Este capítulo cubre la gestión remota (Menú SMT 24.11).

32.1 Descripción de la Gestión Remota

La gestión remota permite determinar a qué servicios/protocolos del Prestige es posible acceder, a través de qué interfaces y desde qué ordenadores.

32.2 Gestión Remota

Para deshabilitar la gestión remota de un servicio, seleccione Disable en el correspondiente campo Server Access. Teclee 11 desde el menú 24 para mostrar el **Menu 24.11 – Remote Management Control**.

32.2.1 Configuración Gestión Remota

Es posible gestionar su Prestige desde una ubicación remota a través de:

Internet (**WAN Only**), LAN (**LAN Only**), LAN y WAN (**All**) o ninguno de los interfaces (**Disable**).

Si habilita la gestión remota de un servicio, pero ha aplicado un filtro que bloquea el servicio, entonces no será posible acceder remotamente al servicio.

Teclee 11, desde el menú 24, para mostrar el **Menu 24.11 – Remote Management Control** (mostrado a continuación).

```
Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                Server Access = LAN only
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                Server Access = LAN only
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                Server Access = LAN only
  Secured Client IP = 0.0.0.0


            Press ENTER to Confirm or ESC to Cancel:
```

Figura 32-1 Menu 24.11 Control de Gestión Remota

La siguiente tabla describe los campos de este menú.

Tabla 32-1 Menu 24.11 Control de Gestión Remota

CAMPO	DESCRIPCIÓN	EJEMPLO
Telnet Server FTP Server Web Server	Cada una de estas etiquetas de *Sólo lectura* indica un servicio que puede utilizar para gestionar remotamente el Prestige.	
Port	Este campo muestra el número de puerto para el servicio de gestión remota. Puede cambiar el número de puerto para un servicio si es necesario, pero debe usar el mismo número de puerto para utilizar ese servicio para gestión remota.	23
Access	Seleccione el interfaz de acceso (si hay alguno) con la [BARRA ESPACIADORA]]. Las opciones son: **LAN only**, **WAN only**, **All** or **Disable** (Sólo LAN, sólo WAN, Todos o Deshabilitado). Por defecto es **LAN only**.	**LAN only**
Secured Client IP	Por defecto pone 0.0.0.0 que permite a cualquier cliente usar este servicio para gestionar remotamente el Prestige. Introduzca una dirección IP para restringir el acceso a un cliente con esa dirección IP.	0.0.0.0
Una vez que haya rellenado este menú, presione [ENTER] en el mensaje "Press ENTER to Confirm or ESC to Cancel" para guardar su configuración, o pulse [ESC] para cancelar.		

32.2.2 Limitaciones de la Gestión Remota

La gestión remota sobre la LAN o la WAN no funcionará si:

1. Hay aplicado algún filtro en el menú 3.1 (LAN) o en el menú 11.5 (WAN) que bloquea el servicio Telnet, FTP o Web.
2. Se ha deshabilitado el servicio en el menú 24.11.
3. La dirección IP del campo Secured Client IP (menú 24.11) no coincide con la IP del cliente. Si no hay coincidencia, el Prestige desconectará la sesión inmediatamente.
4. Existe otra sesión de gestión ejecutándose con igual o mayor prioridad. Únicamente se puede tener una sesión de gestión al mismo tiempo.
5. Hay una regla del firwall que está bloqueando este tráfico.

32.3 Gestión Remota y NAT

Cuando el NAT está habilitado:

- Utilice la dirección IP de la WAN del Prestige cuando esté configurando desde la WAN.
- Utilice la dirección IP de la LAN del Prestige cuando esté configurando desde la LAN.

32.4 Temporizador de Inactividad del Sistema

Hay un temporizador del sistema de cinco minutos (300 segundos). Su Prestige le desconectará del sistema automáticamente si la sesión permanece inactiva durante ese periodo de tiempo, excepto cuando se está continuamente actualizando el estado en el menú 24.1 o cuando se haya modificado el `sys stdio` desde línea de comandos.

Capítulo 33
Políticas de Enrutamiento IP

Este capítulo trata sobre la configuración y aplicación de políticas para el enrutamiento IP.

33.1 Descripción de las Políticas de Enrutamiento IP

Tradicionalmente, el enrutamiento está basado sólo en la dirección de destino y el IAD (Dispositivo Analógico Integrado) toma el camino más corto para enviar un paquete. La Política de Enrutamiento IP (IPPR) proporciona un mecanismo para ignorar el comportamiento de enrutamiento por defecto y modificar el envío de paquetes basándose en la política definida por el administrador de red. El enrutamiento basado en políticas se aplica a paquetes entrantes en cada interfaz por separado, dando prioridad sobre el enrutamiento normal.

33.2 Beneficios de las Políticas de Enrutamiento IP

- Enrutamiento basado en el origen – Los administradores de red pueden utilizar enrutamiento basado en políticas para dirigir el tráfico desde diferentes usuarios a través de diferentes conexiones.
- Calidad de Servicio (QoS) – Las organizaciones pueden diferenciar el tráfico configurando valores de precedencia o ToS (Tipo de Servicio) en la cabecera IP en la periferia de una red para habilitar al backbone priorizar el tráfico.
- Ahorro de coste – IPPR permite a las organizaciones el enviar el posible tráfico interactivo por caminos de alto ancho de banda, alto coste; mientras que el resto del tráfico se transmite por caminos de bajo coste.
- Carga compartida – Los administradores de red pueden utilizar el IPPR para distribuir el tráfico entre múltiples caminos.

33.3 Políticas de Enrutamiento

Las políticas de enrutamiento individuales se usan como parte del proceso global IPPR. Una política define los criterios que debe cumplir un paquete y la acción a llevar a cabo si los cumplen. La acción se lleva a cabo solamente si los criterios se cumplen. Los criterios incluyen la dirección de origen y puerto, el protocolo IP (ICMP, UDP, TCP, etc.), la dirección de destino y puerto, TOS y la prioridad (campos de la

cabecera IP) y longitud. La inclusión del criterio de longitud es para diferenciar entre tráfico interactivo y la mayor parte del tráfico. Las aplicaciones interactivas, por ejemplo, el telnet, tienden a crear paquetes pequeños, mientras que la mayor parte del tráfico, por ejemplo, la transferencia de ficheros, tiende a producir paquetes grandes.

Las acciones a llevar a cabo pueden ser:

- Enrutar el paquete por un gateway diferente (y mejorar el interfaz de salida).
- Configurar los campos ToS y precedencia en la cabecera IP.

IPPR sigue el servicio de filtrado de paquetes del Servidor de Acceso Remoto (RAS) en estilo e implementación. Las políticas están divididas en conjuntos, donde se agrupan las políticas relacionadas. Un usuario define las políticas antes de aplicarlas a un interfaz o nodo remoto, de la misma forma que los filtros. Hay 12 conjuntos de políticas con séis políticas en cada conjunto.

33.4 Configuración de Políticas de Enrutamiento IP

El Menu 25 muestra todas las políticas definidas.

```
                    Menu 25 - IP Routing Policy Setup

      Policy                              Policy
      Set #        Name                   Set #        Name
      ------  -----------------           ------  -----------------
        1      test                          7      _______________
        2      _______________               8      _______________
        3      _______________               9      _______________
        4      _______________              10      _______________
        5      _______________              11      _______________
        6      _______________              12      _______________


                      Enter Policy Set Number to Configure= 0

                      Edit Name= N/A

                      Press ENTER to Confirm or ESC to Cancel:
```

Figura 33-1 Menu 25 Configuración Políticas de Enrutamiento IP

Para configurar una política de enrutamiento, siga el siguiente procedimiento:

Paso 1. Teclee 25 en el menú principal para abrir el **Menu 25 – IP Routing Policy Setup**.

Paso 2. Introduzca el índice de la política que desea configurar para abrir el **Menu 25.1 – IP Routing Policy Setup**.

El menú 25.1 muestra el resumen de un conjunto de políticas, incluyendo los criterios y la acción de una de las políticas del conjunto, y si la política está activa o no. Cada política consta de dos líneas. La primera parte es el criterio del paquete entrante y la última es la acción. Entre estas dos partes, el separador "|" indica que la acción se lleva a cabo cuando se cumplen los criterios y el separador "=" indica que la acción se lleva a cabo cuando no se cumplen dichos criterios.

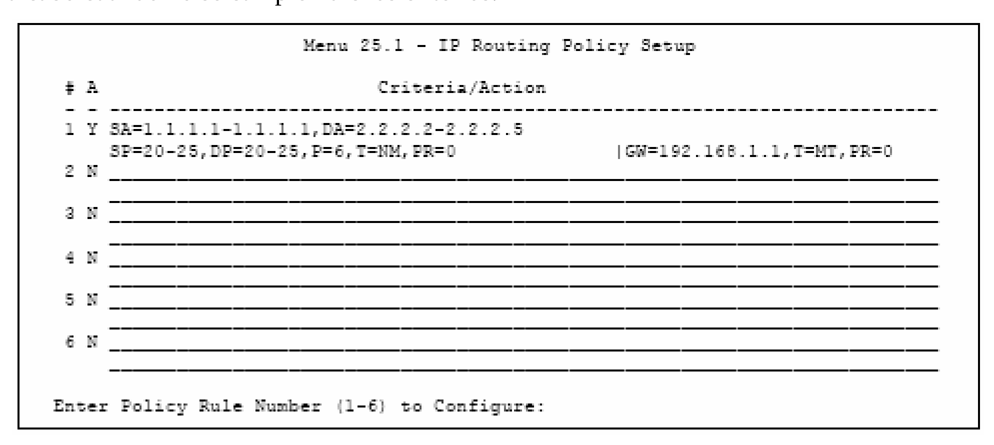


Figura 33-2 Menu 25.1 Configuración Políticas de Enrutamiento IP

Tabla 33-1 Menu 25.1 Configuración Políticas de Enrutamiento IP

ABREVIATURA		SIGNIFICADO
Criterio	SA	Dirección IP de Origen
	SP	Puerto de Origen
	DA	Dirección IP de Destino
	DP	Puerto de Destino
	P	Número del protocolo IP de capa 4 (TCP=6, UDP=17…)
	T	Tipo de servicio del paquete entrante
	PR	Prioridad del paquete entrante
Acción	GW	Dirección IP del Gateway
	T	Tipo de servicio de salida
	P	Prioridad de salida
Servicio	NM	Normal
	MD	Retraso mínimo

MT	Flujo máximo
MR	Máxima fiabilidad
MC	Mínimo coste

Introduzca un número de 1 a 16 para mostrar el Menu 25.11 – IP Routing Policy (ver siguiente figura). Este menú permite configurar una política.

```
                         Menu 25.1.1 - IP Routing Policy

           Policy Set Name= test
           Active= Yes
           Criteria:
             IP Protocol    = 6
             Type of Service= Normal          Packet length= 40
             Precedence     = 0                 Len Comp= N/A
             Source:
               addr start= 1.1.1.1            end= 1.1.1.1
               port start= 20                 end= 20
             Destination:
               addr start= 2.2.2.2            end= 2.2.2.2
               port start= 20                 end= 20
           Action= Matched
             Gateway addr   = 192.168.1.1     Log= No
             Type of Service= Max Thruput
             Precedence     = 0

                               Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figura 33-3 Menu 25.1.1 Política de Enrutamiento IP

La siguiente tabla describe los campos de este menú.

Tabla 33-2 Menu 25.1.1 Política de Enrutamiento IP

CAMPO	DESCRIPCIÓN
Policy Set Name	Es el nombre del conjunto de políticas del **Menu 25 – IP Routing Policy Setup**.
Active	Presione la [BARRA ESPACIADORA] y luego [INTRO] para seleccionar **Yes** para activar o **No** para desactivar la política. La políticas inactivas se muestran con un signo menos “-“ en el menú SMT 25.
Criteria	
IP Protocol	Protocolo IP de nivel 4, por ejemplo, **UDP**, **TCP**, **ICMP**, etc.
Type of Service	Priorizar el tráfico de red entrante seleccionando **Don’t Care**, **Normal**, **Min Delay**, **Max Throughput, Min Cost** o **Max Reliable** (No importa, Normal, Mínimo Retraso, Máximo Flujo, Mínimo Coste o Máxima Fiabilidad).

Precedence	El valor de prioridad del paquete entrante. Presione la [BARRA ESPACIADORA] y luego [INTRO] para seleccionar un valor de **0** a **7** o **Don't Care** (No importa).
Packet Length	Teclee la longitud de los paquetes entrantes (en bytes). Los operadores en el campo **Len Comp** (siguiente campo) se aplicarán a los paquetes de esta longitud.
Len Comp	Presione la [BARRA ESPACIADORA] y luego [INTRO] para seleccionar **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal** (Igual, Distinto, Menor, Mayor, Menor o Igual, o Mayor o Igual).
Source:	
addr start / end	Rango de direcciones IP de origen (de principio a fin).
port start / end	Rango de números de puerto de origen (de principio a fin); aplicable solamente para TCP/UDP.
Destination:	
addr start / end	Rango de direcciones IP de destino (de principio a fin).
port start / end	Rango de números de puerto de destino (de principio a fin); aplicable solamente para TCP/UDP.
Action	Especifica si una acción debe llevarse a cabo cuando cumple los criterios (**Matched**) o cuando no los cumple (**Not Matched**).
Gateway addr	Es la dirección del gateway de salida. El gateway debe estar en la misma subred que el Prestige si está en la LAN, si no, el gateway debe tener la dirección IP de un nodo remoto. Por defecto pone 0.0.0.0.
Type of Service	Establezca el nuevo valor del TOS del paquete de salida. Priorice el tráfico de red entrante seleccionando **No Change**, **Normal**, **Min Delay**, **Max Throughput**, **Max Reliable** or **Min Cost** (Sin Cambio, Normal, Mínimo Retraso, Máximo Flujo, Máxima Fiabilidad o Mínimo Coste).
Precedence	Ponga el valor de prioridad de los nuevos paquetes de salida. Los valores son de **0** a **7** o **No Change** (Sin cambio).
Log	Presione la [BARRA ESPACIADORA] y luego [INTRO] para seleccionar **Yes** para hacer una entrada en el registro del sistema cuando se ejecuta una política.
Cuando se haya completado este menú, presione [ENTER] en el mensaje "Press ENTER to confirm or ESC to cancel" para guardar su configuración o [ESC] para cancelar y volver a la pantalla anterior.	

33.5 Aplicación de una Política IP

Esta sección muestra dónde aplicar las políticas IP tras haberlas diseñado.

33.5.1 Políticas IP Ethernet

En el **Menu 3 — Ethernet Setup**, teclee 2 para ir al **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**.

Puede seleccionar hasta cuatro conjuntos de políticas IP (de 12) tecleando sus números separados por comas, por ejemplo, 2, 4, 7, 9.

```
                 Menu 3.2 - TCP/IP and DHCP Ethernet Setup

        DHCP Setup:
          DHCP= None
          Client IP Pool Starting Address= N/A
          Size of Client IP Pool= N/A
          Primary DNS Server= N/A
          Secondary DNS Server= N/A
          Remote DHCP Server= N/A
        TCP/IP Setup:
          IP Address= 192.168.1.1
          IP Subnet Mask= 255.255.255.0
          RIP Direction= Both
            Version= RIP-2B
          Multicast= IGMP-v2
          IP Policies= 2,4,7,9
          Edit IP Alias= No

                  Press ENTER to Confirm or ESC to Cancel:
```

Introduzca aquí las políticas IP

Figura 33-4 Menu 3.2 Configuración TCP/IP y DHCP

Vaya al menú 11.3 (que se muestra a continuación) y teclee el número(s) de los conjunto(s) de Políticas de Enrutamiento IP que considere oportunos. Puede encadenar hasta cuatro conjuntos de políticas tecleando sus números separados por comas.

```
              Menu 11.3 - Remote Node Network Layer Options

   IP Options:                          Bridge Options:
     IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
     Rem IP Addr: 0.0.0.0
     Rem Subnet Mask= 0.0.0.0
     My WAN Addr= 0.0.0.0
     NAT= Full Feature
       Address Mapping Set= 2
     Metric= 2
     Private= No
     RIP Direction= Both
       Version= RIP-2B
     Multicast= IGMP-v2
     IP Policies= 2,4,7,9

 Press ENTER to Confirm or ESC to Cancel:
```

Introduzca aquí las políticas IP

Figura 33-5 Menu 11.3 Opciones de Red del Nodo Remoto

33.6 Ejemplo de Políticas de Enrutamiento IP

Si una red tiene conexiones tanto a Internet como a nodos remoto, puede enrutar paquetes Web a Internet usando una política y enrutar paquetes FTP hacia una red remota usando otra política. Vea la figura siguiente.

La ruta 1 representa la ruta IP por defecto y la ruta 2 representa la ruta IP configurada.

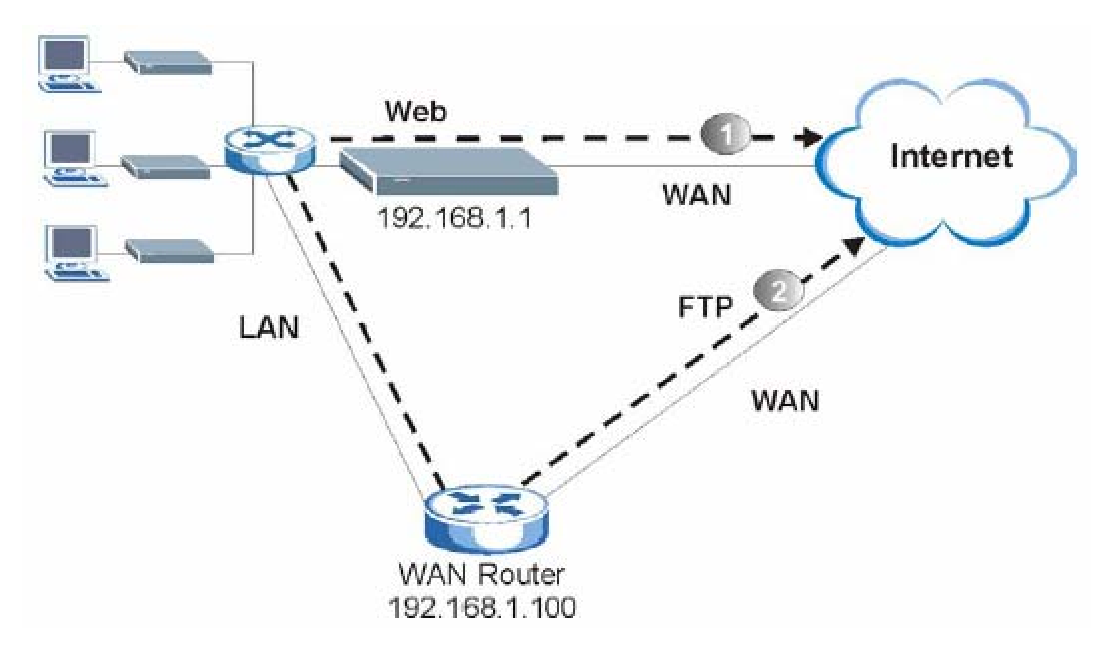


Figura 33-6 Ejemplo de Políticas de Enrutamiento IP

Para forzar a los paquetes Web que vienen de los clientes con direcciones IP de 192.168.1.33 a 192.168.1.64 a ser enrutados a Internet a través del puerto WAN del Prestige, siga los pasos indicados a continuación:

Paso 1. Crear una polítca de enrutamiento en el menú 25.

Paso 2. Crear una regla para este conjunto en el **Menu 25.1.1 – IP Routing Policy** como se muestra.

```
                         Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set1
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care         Packet length= 10
            Precedence     = Don't Care           Len Comp= N/A
            Source:
              addr start= 192.168.1.33     end= 192.168.1.64
              port start= 0                end= N/A
            Destination:
              addr start= 0.0.0.0              end= N/A
              port start= 80                   end= 80
          Action= Matched
            Gateway addr   = 192.168.1.1        Log= No
            Type of Service= No Change
            Precedence     = No Change

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figura 33-7 Ejemplo de Política de Enrutamiento IP

Paso 3. Compruebe el **Menu 25.1 – IP Routing Policy Setup** para ver si la reglas se ha añadido correctamente.

Paso 4. Crear otra política en el menú 25.

Paso 5. Crear una regla en el menú 25.1 para este conjunto para enrutar los paquetes desde cualquier host (IP=0.0.0.0 significa cualquier máquina) con protocolo TCP y puerto de acceso FTP a través de otro gateway (192.168.1.100).

```
                         Menu 25.1.1 - IP Routing Policy

           Policy Set Name= set2

           Active= Yes
           Criteria:
             IP Protocol    = 6
             Type of Service= Don't Care            Packet length= 10
             Precedence     = Don't Care              Len Comp= N/A
             Source:
               addr start= 0.0.0.0                  end= N/A
               port start= 0                        end= N/A
             Destination:
               addr start= 0.0.0.0                  end= N/A
               port start= 20                       end= 21
           Action= Matched
             Gateway addr  =192.168.1.100           Log= No
             Type of Service= No Change
             Precedence     = No Change

                    Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
```

Figura 33-8 Ejemplo de Política de Enrutamiento IP

Paso 6. Compruebe en el Menu 25.1 – IP Policy Routing Setup que la regla se ha añadido correctamente.

Paso 7. Aplique ambas políticas en el menú 3.2 como se indica.

```
                     Menu 3.2 - TCP/IP and DHCP Ethernet Setup

                      DHCP Setup
                        DHCP= Server
                        Client IP Pool Starting Address= 192.168.1.33
                        Size of Client IP Pool= 64
                        Primary DNS Server= 0.0.0.0
                        Secondary DNS Server= 0.0.0.0
                        Remote DHCP Server= N/A
                      TCP/IP Setup:
                        IP Address= 192.168.1.1
                        IP Subnet Mask= 255.255.255.0
                        RIP Direction= Both
                          Version= RIP-1
                        Multicast= None
                        IP Policies= 1,2
                        Edit IP Alias= No

                      Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Figura 33-9 Ejemplo de Aplicación de Políticas IP

Capítulo 34
Programación de Llamadas

La programación de llamadas (applicable únicamente para encapsulaciones PPPoA o PPPoE) permite configurar cuando debe ser llamado un nodo remoto y por cuánto tiempo.

34.1 Introducción

La característica de programación de llamadas le permite al Prestige gestionar un nodo remoto y ordenar cuando un nodo remoto debe ser llamado y por cuanto tiempo. Es una característica similar a la de programación de un vídeo (puede especificar un periodo de tiempo durante el cual el vídeo grabará). Puede aplicar hasta 4 conjuntos de programas en el **Menu 11.1 — Remote Node Profile**. En el menú principal, teclee 26 para acceder al **Menu 26 — Schedule Setup** que se ve a continuación.

```
                         Menu 26 - Schedule Setup

   Schedule                              Schedule
    Set #        Name                     Set #            Name
   ------   -----------------            ------     ------------------
      1      ______________                 7         ______________
      2      ______________                 8         ______________
      3      ______________                 9         ______________
      4      ______________                10         ______________
      5      ______________                11         ______________
      6      ______________                12         ______________

                  Enter Schedule Set Number to Configure=

                  Edit Name=

                  Press ENTER to Confirm or ESC to Cancel:
```

Figura 34-1 Menu 26 Configuración Programación de Llamadas

Los conjuntos con números más bajos tienen prioridad sobre los que tienen números más altos evitando de ese modo los conflictos de programación. Por ejemplo, si los conjuntos 1, 2 ,3 y 4 se aplican en el nodo remoto, entonces el conjunto 1 tendrá preferencia sobre los conjuntos 2, 3 y 4 ya que el Prestige, por defecto, aplica el conjunto con número más bajo primero. El conjunto 2 tendrá preferencia sobre el 3 y el 4, y así sucesivamente.

Puede diseñar hasta 12 conjuntos de programas pero solamente puede aplicar hasta cuatro a un nodo remoto.

Para borrar un conjunto de programas, introduzca el número de conjunto y pulse la [BARRA ESPACIADORA] **e** [INTRO] **(o borrar) en el campo** Edit Name**.**

Para configurar un conjunto de programación, seleccione el conjunto que quiere configurar en el menú 26 (1-12) y pulse [INTRO] para ver el **Menu 26.1 — Schedule Set Setup** como se muestra.

```
                    Menu 26.1 - Schedule Set Setup

          Active= Yes
          Start Date(yyyy/mm/dd) = 2000 - 01 - 01
          How Often= Once
          Once:
            Date(yyyy/mm/dd)= 2000 - 01 - 01
          Weekdays:
            Sunday= N/A
            Monday= N/A
            Tuesday= N/A
            Wednesday= N/A
            Thursday= N/A
            Friday= N/A
            Saturday= N/A
          Start Time (hh:mm)= 00 : 00
          Duration (hh:mm)= 00 : 00
          Action= Forced On

                   Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle
```

Figura 34-2 Menu 26.1 Configuración Programación de Llamadas

Si una conexión ya ha sido establecida, el Prestige no la desconectará. Una vez la conexión se desconecte bien manualmente o bien porque expire el temporizador, entonces el nodo remoto no podrá ser llamado hasta el final del campo **Duración (Duration)**.

Tabla 34-1 Menu 26.1 Configuración Programación de Llamadas

CAMPO	DESCRIPCIÓN	EJEMPLO
Active	Presione la [BARRA ESPACIADORA] para seleccionar **Yes** o **No**. **Yes** e [INTRO] para activar el conjunto de programación.	**Yes**
Start Date	Introduzca la fecha de inicio cuando desee que tenga efecto en formato año-mes-día. Las fechas válidas son del presente al 2036-Febrero-5.	2000-01-01
How Often	Debe este conjunto de programación repetirse semanalmente o debe usarse solamente una vez? Pulse [BARRA ESPACIADORA] e [INTRO] para seleccionar **Once** (una vez) o **Weekly** (semanalmente). Estas dos opciones se excluyen mutuamente. Si	**Once**

	Once está seleccionada, todas las configuraciones de días de la semana están **N/A**. En ese caso, la regla de programas se borra automáticamente después de que el tiempo asignado ha transcurrido.	
Once: Date	Si ha seleccionado **Once** en el campo anterior **How Often**, introduzca la fecha en debería activarse el conjunto aquí en formato año-mes-día.	2000-01-01
Weekday: Day	Si ha seleccionado **Weekly** en el campo anterior **How Often**, seleccione el día(s) que deba activarse (y repetirse) pulsando la [BARRA ESPACIADORA] para seleccionar **Yes**, luego pulse [INTRO].	**Yes** **No** **N/A**
Start Time	Introduzca la hora de inicio cuando desee el conjunto de programas cuando van a tener efecto en formato hora-minuto.	09:00
Duration	Introduzca la longitud máxima del tiempo permitida para la conexión en formato hora-minuto.	08:00
Action	**Forced On** significa que la conexión se mantiene haya o no una llamada en la línea y persiste un periodo de tiempo especificado en el campo **Duration**. **Forced Down** indica que la conexión se bloquea haya o no haya llamada en la línea. **Enable Dial-On-Demand** indica que esta programación permite una llamada de petición en la línea. **Disable Dial-On-Demand** impide que haya llamadas de petición en la línea.	**Forced On**
Cuando haya completado en este menú, pulse [ENTER] en el mensaje “Press ENTER to confirm or ESC to cancel” para guardar su configuración o pulse [ESC] para cancelar y volver a la pantalla anterior.		

Una vez que los conjuntos de programas estén configurados, debe aplicarlos a los nodos deseados. Teclee 11 en el **Main Menu** e introduzca el índice del nodo remoto al que le quiere aplicar el conjunto. Usando [BARRA ESPACIADORA], seleccione **PPPoE** o **PPPoA** en el campo **Encapsulation** y luego pulse [INTRO] para hacer disponible el campo de conjuntos de programaciones como se ve a continuación.

```
                    Menu 11.1 - Remote Node Profile

     Rem Node Name= ChangeMe              Route= IP
     Active= Yes                          Bridge= No

     Encapsulation= PPPoE                 Edit IP/Bridge= No
     Multiplexing=VC-based                Edit ATM Options= No
     Service Name=                        Telco Option:
     Incoming                               Allocated Budget(min)= 0
       Rem Login=                           Period(hr)= 0
       Rem Password= ********               Schedules= 1,2,3,4
     Outgoing=                              Nailed-Up Connection= No
       My Login=?
       My Password= ********              Session Options:
       Authen= CHAP/PAP                     Edit Filter Sets= No
                                            Idle Timeout(sec)= 100


                Press ENTER to Confirm or ESC to Cancel:


Press Space Bar to Toggle.
```


Figura 34-3 Aplicación de los Programas de Llamadas en un Nodo Remoto (PPPoE)

Puede aplicar hasta cuatro conjuntos de programas, separados por comas, para un nodo remoto. Cambie los números de conjunto de programa según sus prioridades.

Capítulo 35
SPTGEN Interno

35.1 Descripción SPTGEN Interno

El SPTGEN interno es un fichero editable de configuración muy útil para la configuración eficiente de múltiples Prestige. El SPTGEN interno permite configurar, guardar y actualizar múltiples menús simultáneamente utilizando un único fichero editable de configuración – eliminando la necesidad de navegar y configurar cada menú SMT del Prestige de forma individual.

35.2 Formato del Fichero Editable de Configuración

Todos los campos del fichero editable STPGEN siguen el siguiente formato:

<número de identificación del campo = nombre del campo = valores permitidos del parámetro = entrada>,

Donde <entrada> es el valor del parámetro acorde con los valores permitidos para el mismo.

La siguiente figura un ejemplo de fichero SPTGEN.

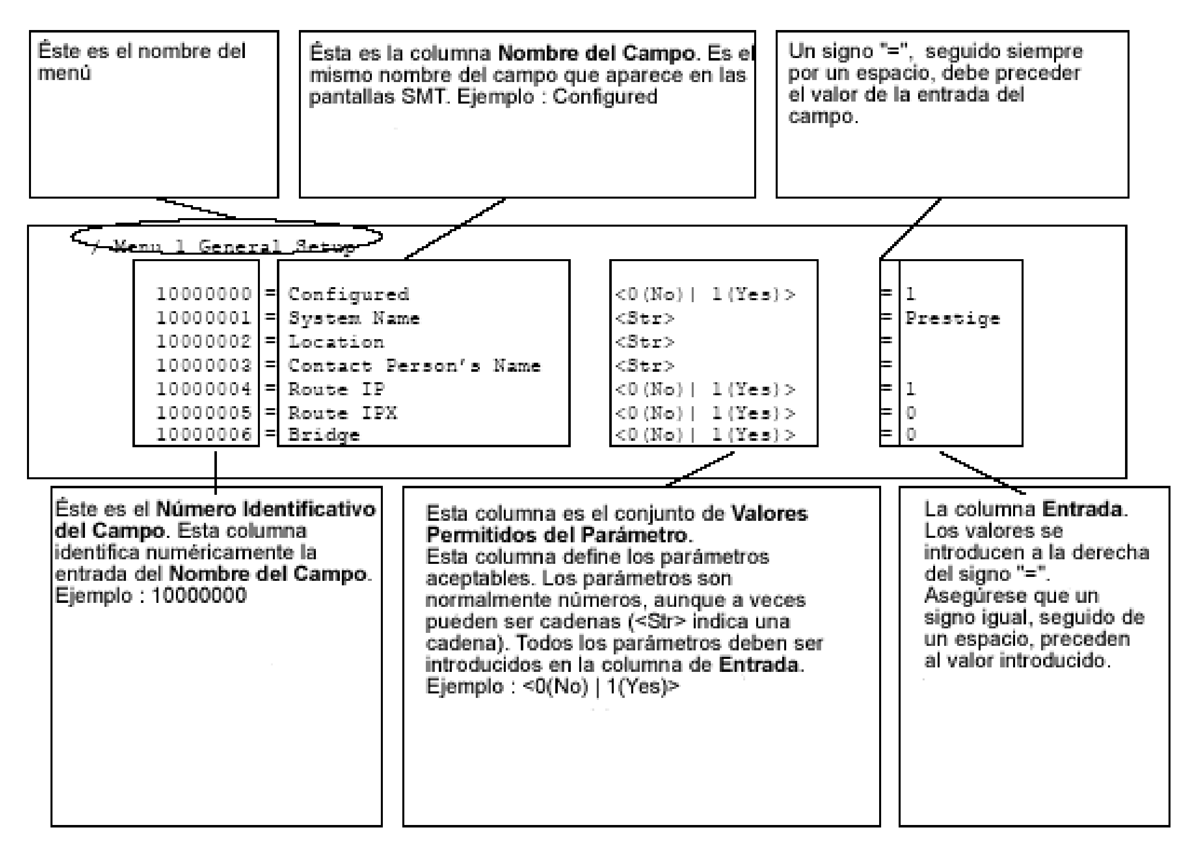


Figura 35-1 Formato del Fichero de Configuración : Descripción por Columnas

NO altere o elimine ningún campo excepto los parámetros de la columna *Valor*.

35.2.1 Modificaciones del Fichero SPTGEN – Puntos Importantes

- Cada parámetro debe ser introducido precedido por un signo “=” y un espacio.
- Algunos parámetros dependen de otros. Por ejemplo, si se deshabilita el campo **Configured** en el menu 1 (ver Figura 35-1), entonces se deshabilitarán todos los campos de este menú.
- Si se introduce un parámetro inválido en la columna **Entrada**, el Prestige no guardará la configuración.

35.3 Ejemplo de Descarga del Fichero SPTGEN mediante FTP

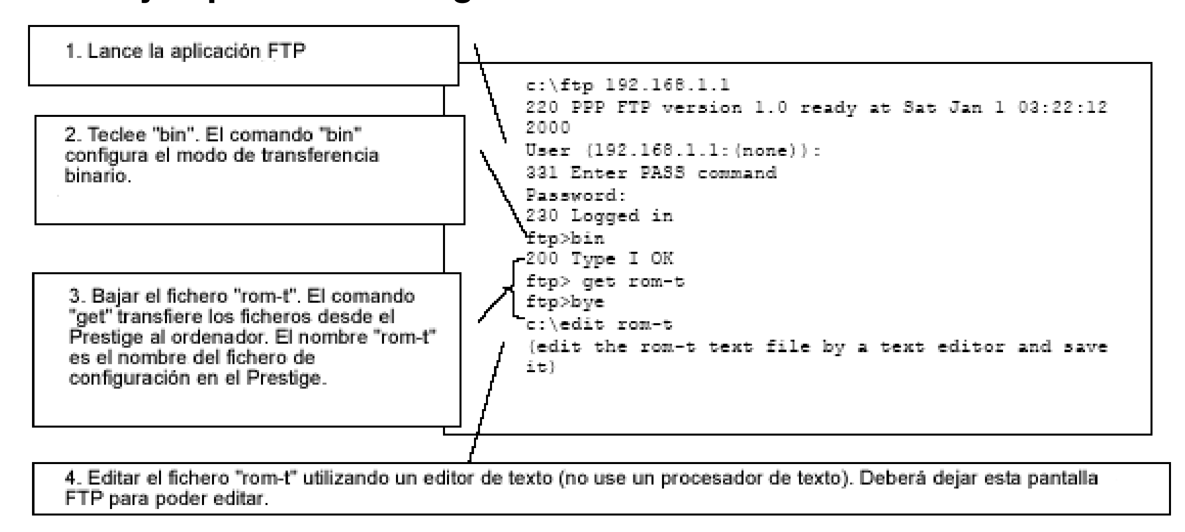


Figura 35-2 Ejemplo de Descarga del Fichero SPTGEN via FTP

Puede renombrar el fichero “rom-t” para almacenarlo en su ordenador pero debe ser renombrado nuevamente como “rom-t” al subirlo al Pretige.

35.4 Ejemplo de Carga del Fichero SPTGEN mediante FTP

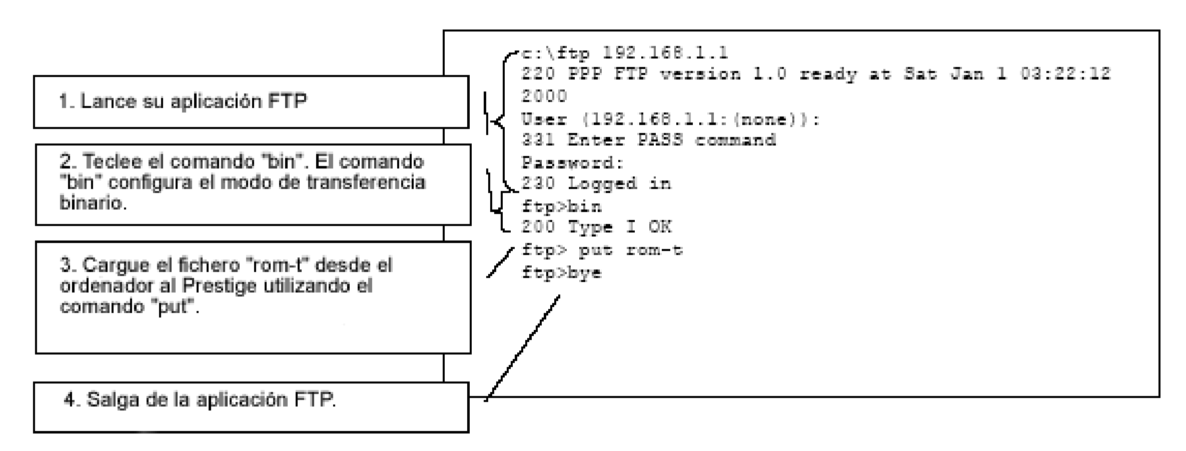


Figura 35-3 Ejemplo de Carga de Fichero SPTGEN via FTP

Apéndice A

Resolución de Problemas

Este capítulo cubre problemas potenciales y sus correspondientes soluciones.

Problemas con la puesta en marcha del Prestige

Tabla A-1 Resolución de Problemas con la puesta en marcha del Prestige

PROBLEMA	ACCIÓN CORRECTIVA
Ninguno de los LEDs se enciende al conectar el Prestige	Asegúrese que el adaptador de corriente del Prestige está correctamente conectado al Prestige y enchufado a una toma de corriente apropiada. Compruebe que tanto el Prestige como la fuente de alimentación están conectados. Apague y encienda el Prestige. Si el error persiste, podría tratarse de un problema hardware. En este caso, deberá contactar con su vendedor.

Problemas con el LED de LAN

Tabla A-2 Resolución de Problemas del LED de LAN

ETIQUETA	ACCIÓN CORRECTIVA
El LED de LAN no se enciende	Compruebe las conexiones y tipo del cable Ethernet. Asegúrese de la ausencia de problemas en el cable. Verifique que la tarjeta Ethernet funciona correctamente.

Problemas con el LED DSL

Tabla A-3 Resolución de problemas con el LED DSL

PROBLEMA	ACCIÓN CORRECTIVA
El LED DSL está apagado.	Compruebe el cable y las conexiones entre el puerto DSL del Prestige y la

	roseta telefónica. Asegúrese que la compañía telefónica ha comprobado su línea telefónica y la ha configurado para el servicio DSL. Reinicie su línea ADSL para iniciar el enlace con el DSLAM. Para más detalles, consulte con el capítulo de Mantenimiento.

Problemas con el Interfaz LAN

Tabla A-4 Resolución de problemas del interfaz LAN

PROBLEMA	ACCIÓN CORRECTIVA
No es posible acceder al Prestige desde la LAN	Si el LED 10/100M en el panel frontal está apagado, consulte la tabla A-2 acerca de los problemas con el LED de LAN. Asegúrese que la dirección IP y la máscara de subred en el Prestige y en el ordenador(es) están dentro de la misma subred.
No es posible hacer ping a ninún ordenador de la LAN	Si el LED 10/100M en el panel frontal está apagado, consulte la tabla A-2 acerca de los problemas con el LED de LAN. Compruebe que la dirección IP y máscara de subred del Prestige y de los ordenadores están dentro de la misma subred.

Problemas con el Interfaz WAN

Tabla A-5 Resolución de problemas con el interfaz WAN

PROBLEMA	ACCIÓN CORRECTIVA
No es posible obtener una dirección IP en la WAN desde el ISP.	El ISP proporciona la dirección IP a la WAN tras el proceso de autenticación. La autenticación se hace a través del nombre de usuario y contraseña, dirección MAC o el nombre de host. El nombre de usuario y contraseña se aplican sólo a encapsulación PPPoE y PPPoA. Asegúrese que ha introducido correctamente el **Service Type, User Name** y **Password**.

Problemas con el Acceso a Internet

Tabla A-6 Resolución de problemas con el Acceso a Internet

PROBLEMA	ACCIÓN CORRECTIVA
No es posible acceder a Internet.	Asegúrese que el Prestige está encendido y conectado a la red. Si el LED DSL está apagado, consulte la Tabla A-3 de Resolución de problemas. Verifique sus parámetros WAN. Asegúrese que ha introducido los valores correctos de nombre de usuario y contraseña. Si está utilizando PPPoE pass-through, asegúrese que el brige está activado. Para estaciones wireless, compruebe que tanto el Prestige como las estaciones wireless están utilizando el mismo ESSID, canal y claves WEP (en caso de tener la encriptación activada).
La conexión a Internet se desconecta.	Compruebe las reglas de horario de conexión. Si se utiliza encapsulación PPPoA o PPPoE, compruebe el valor del temporizador de inactividad. Contacte con su ISP.

Problemas con la Contraseña

Tabla A-7 Resolución de Problemas con la Contraseña

PROBLEMA	ACCIÓN CORRECTIVA
No es posible acceder al Prestige	El nombre de usuario es “admin.”. La contraseña por defecto es “1234”. Los campos del nombre de usuario y contraseña distinguen entre mayúsculas y minúsculas. Asegúrese que se introduce el nombre de usuario y contraseña correctos. Si se ha modificado la contraseña y la ha olvidado, será necesario restaurar la configuración por defecto. Esto restaurará todos los parámetros por defecto incluida la contraseña.

Problemas con el Configurador Web

Tabla A-8 Resolución de Problemas con el Configurador Web

PROBLEMA	ACCIÓN CORRECTIVA
No es posible acceder al configurador web.	Consulte la Tabla A-7 acerca de la Resolución de Problemas para la Contraseña. Asegúrese que no existe ningún sesión SMT ejecutándose. Compruebe que ha habilitado el acceso a través de Telnet. Si se ha configurado una dirección de confianza, la dirección IP desde la que accede debe coincidir con ésta. Consulte el apartado de Gestión Remota para más detalles. Para el acceso desde WAN, es necesario configurar la gestión remota para permitir el acceso desde la Wan (o desde todos los interfaces). Las direcciones IP del Prestige y del ordenador deben estar dentro del mismo rango de red para acceso desde la LAN. Si ha modificado la dirección IP LAN del Prestige, introduzca esta nueva dirección IP en el URL. Elimine cualquier filtro en el menú 3.1 (LAN) o 11.5 (WAN) que pueda bloquear el acceso web. Consulte también el apartado relacionado con la Resolución de Problemas con la Gestión Remota.

Problemas con la Gestión Remota

Tabla A-9 Resolución de Problemas con la Gestión Remota

PROBLEMA	ACCIÓN CORRECTIVA
No es posible gestionar el equipo ni por WAN ni por LAN	Consulte la sección de Limitaciones de la Gestión Remota para ver los escenarios donde la gestión no es posible. Utilice la dirección IP de la WAN del Prestige cuando intente acceder desde la WAN Utilice la dirección IP de la LAN del Prestige cuando intente acceder desde la LAN Consulte la Tabla A-4 relativa a problemas en el interfaz LAN para ver instrucciones de chequeo de la LAN

	Consulte la sección de problemas relacionados con la interfaz WAN para ver instrucciones de chequeo de la conexión WAN Vea también el apartado relacionado con problemas en el configurador web.

Apéndice B
Subredes IP

Direccionamiento IP

Los routers enlutan el tráfico basándose en un número de red. El rotuer distribuye los paquetes de datos a los hosts correctos utilizando el identificador del host.

Clases IP

Una dirección IP está formada por 4 octetos (8 bits), escritos en formato decimal, por ejemplo, 192.168.1.1 Las direcciones IP están categorizadas en diferentes clases. La clase de una dirección dependerá del valor de sus primeros octetos.

- Direcciones Clase “A” tienen un 0 en el bit más a la izquierda. En la dirección clase “A”, el primer octeto es el número de red y el resto de los 3 octetos se refieren al identificador del host.
- Direcciones Clase “B” tienen un 1 en el bit más a la izquierda y 0 en el siguiente bit más a la izquierda. En una dirección clase “B” los primeros dos octetos hacen referecia al número de red y los dos restantes al identificador de host.
- Direcciones Clase “C” comienzan (empezando desde la izquierda) con 1 1 0. En las direcciones clase “C” los primeros tres octetos hacen referencia al número de red y el último octeto al identificador de host.
- Direcciones Clase “D” comienzan por 1 1 1 0. Las direcciones clase “D” son utilizadas para multicasting. (Existe también una dirección clase “E”. Reservada para uso futuro).

Tabla B-1 Clases de Direcciones IP

DIRECCIÓN IP		**OCTETO 1**	**OCTETO 2**	**OCTETO 3**	**OCTETO 4**
Clase A	0	Número de red	Identificador Host	Identificador Host	Identificador Host
Clase B	10	Número de red	Número de red	Identificador Host	Identificador Host
Clase C	110	Número de red	Número de red	Número de red	Identificador Host

Los identificadores de host con todo ceros o todo unos no está permitido.

Además :

- Una red Clase "C" (8 bits para hosts) podrá tener 2^{8} -2 ó 254 hosts
- Una red Clase "B" (16 bits para hosts) podrá tener 2^{16} -2 ó 65534 hosts
- Una red Clase "A" (24 bits para hosts) podrá tener 2^{24} -2 hosts (aproximadamente 16 millones de hosts).

Como el primer octeto de una dirección IP clase "A" debe contener "0", el primer octeto de una dirección clase "A" tendrá un valor entre 0 y 127.

De forma análoga, el primer octeto de una clase "B" debe empezar con "10", con lo que el primer octeto de una dirección clase "B" tendrán un rango entre 128 y 191. El primer octeto de una dirección clase C comienza por "110", lo que conlleva que pertenecerá al rango 192 a 223.

Tabla B-2 Rangos de IP permitidos por clases

CLASE	RANGO PERMITIDO PARA EL PRIMER OCTETO (BINARIO)	RANGO PERMITIDO PARA EL PRIMER OCTETO (DECIMAL)
Clase A	**0**0000000 a **0**1111111	0 a 127
Clase B	**10**000000 a **10**111111	128 a 191
Clase C	**110**00000 a **110**11111	192 a 223
Clase D	**1110**0000 a **1110**1111	224 a 239

Máscaras de subred

Una máscara de subred se utiliza para determinar los bits que pertenecen al número de red y los bits que forman parte del identificador del host (utilizando una operación AND lógica). Una máscara de subred tiene 32 bits; cada bit de la máscara corresponde con un bit de la dirección IP. Si un bit en la máscara de subred es un "1" entonces el correpondiente bit de la dirección IP es parte del número de red. Si un bit en la máscara de subred es "0", entonces el correspondiente bit de la dirección IP es parte del identificador de host.

Las máscaras de subred se expresan en notación decimal tal como las direcciones IP. Las máscaras "naturales" para las direcciones IP de las clases A,B y C son :

Tabla B-3 Máscaras “Naturales”

CLASE	MÁSCARA NATURAL
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subredes

Con las subredes, la clase acordada para una dirección IP es ignorada. Por ejemplo, una dirección de la clase C no siempre tiene 24 bits para el número de red y 8 bits para el identificador de host. Con las subredes, algunos bits del identificador de hosts pueden convertirse en bits del número de red. Por convención, las máscaras de subred siempre consisten en una secuencia continua de unos seguida por una secuencia seguida de ceros, para un total de 32 bits.

Con esta notación, es fácil especificar el número de unos en lugar de escribir el valor de cada octeto. Esto es normalmente especificado notando una “/” seguida por el número de bits unos en la máscara tras la dirección.

Por ejemplo, 192.1.1.0/25 es equivalente a decir 192.1.1.0 con máscara 255.255.255.128.

La siguiente tabla muestra todas las posibles máscaras de subred para la dirección clase “C” utilizando ambas notaciones.

Tabla B-4 Notación Alternativa Máscara de Subred

MÁSCARA SUBRED	MÁSCARA SUBRED BITS “1”	VALOR BIT ÚLTIMO OCTETO
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

La primera máscara mostrada es la máscara natural de clase “C”. Normalmente si no se especifica la máscara, se entiende que la máscara a usar será la natural.

Ejemplo : Dos Subredes

Como ejemplo, se tiene una dirección 192.168.1.0 clase “C” con máscara de subred 255.255.255.0.

	NÚMERO DE RED	**IDENTIFICADOR DE HOST**
Dirección IP	192.168.1	0
Dirección IP (Binario)	11000000.10101000.00000001	00000000
Máscara de Subred	255.255.255	0
Máscara de Subred (Binario)	11111111.11111111.11111111	00000000

Los tres primeros octetos de la dirección forman el número de red (clase “C”). Se desea disponer de dos redes serparadas.

Dividir la red 192.168.1.0 en dos subredes separadas convirtiendo uno de los bits del identificador de host de la dirección IP como bit del número de red. El bit del Host ID “prestado” puede ser “0” o “1” lo que origina dos subredes; 192.168.1.0 con máscara 255.255.255.128 y 192.168.1.128 con máscara 255.255.255.128.

En la siguiente tabla, los valores de bit del último octeto en negrita indican los bits del identificador de host “prestados” a los bits del número de red. El número de bits del Host ID “prestados” determinan el número de subredes que se pueden tener. El número restante de bits del identificador de host (tras el “préstamo”) determinan el número de hosts que podrá tener cada subred.

Tabla B-5 Subred 1

	NÚMERO DE RED	VALOR BIT ÚLTIMO OCTETO
Dirección IP	192.168.1	0
Dirección IP (Binario)	11000000.10101000.00000001	**0**0000000
Máscara de subred	255.255.255	128
Máscara de subred (Binario)	11111111.11111111.11111111	**1**0000000
Dirección de Subred : 192.168.1.0	ID Host más bajo : 192.168.1.1	
Dirección de Broadcast : 192.168.1.127	ID Host más alto : 192.168.1.126	

Tabla B-6 Subred 2

	NÚMERO DE RED	VALOR BIT ÚLTIMO OCTETO
Dirección IP	192.168.1	128
Dirección IP (Binario)	11000000.10101000.00000001	**1**0000000
Máscara de subred	255.255.255	128
Máscara de subred (Binario)	11111111.11111111.11111111	**1**0000000
Dirección de Subred : 192.168.1.128		ID Host más bajo : 192.168.1.129
Dirección de Broadcast : 192.168.1.255		ID Host más alto : 192.168.1.254

Los 7 bits restantes determinan el número de hosts de cada subred. Los identificadores de host con todo ceros indican la dirección de subred en sí misma y los identificadores de host con todo a unos son la dirección de broadcast de la subred, de manera que el número de hosts disponible para cada subred en el ejemplo anterior sería 2^7 -2 ó 126 hosts para cada subred.

192.168.1.0 con máscara 255.255.255.128 es la subred en sí, y 192.168.1.127 con máscara 255.255.255.128 es la dirección de broadcast para la primera subred. Adiconalmente, la dirección IP más baja que puede ser asignada a un host de la primera subred es 192.168.1.1 y la dirección más alta es 192.168.1.126. De forma similar el rango del identificador de host para la segunda subred sería 192.168.1.129 a 192.168.1.254.

Ejemplo : Cuatro Subredes

El ejemplo anterior ilustra la utilización de una máscara de subred de 25 bits para dividir una dirección clase “C” en dos subredes. De forma similar para dividir una dirección clase “C” en 4 subredes, es necesario “prestar” dos bits del identificador de host para poder formar cuatro posibles combinaciones de 00,01,10 y 11. La máscara de subred sería de 26 bits (11111111.11111111.1111111.**11**000000) o 255.255.255.192. Cada subred contiene 6 bits para el identificador del host, dando lugar a 2^6 -2 ó 62 hosts para cada subred (todo a 0, indica la red en sí y todo a 1 sería la dirección de broadcast).

Tabla B-7 Subred 1

	NÚMERO DE RED	**VALOR BIT ÚLTIMO OCTETO**
Dirección IP	192.168.1	0

Dirección IP (Binario)	11000000.10101000.00000001	**00**000000
Máscara de subred (Binario)	11111111.11111111.11111111	**11**000000
Dirección de Subred : 192.168.1.0	ID Host más bajo : 192.168.1.1	
Dirección de Broadcast : 192.168.1.63	ID Host más alto : 192.168.1.62	

Tabla B-8 Subred 2

	NÚMERO DE RED	**VALOR BIT ÚLTIMO OCTETO**
Dirección IP	192.168.1	64
Dirección IP (Binario)	11000000.10101000.00000001	**01**000000
Máscara de subred (Binario)	11111111.11111111.11111111	**11**000000
Dirección de Subred : 192.168.1.64	ID Host más bajo : 192.168.1.65	
Dirección de Broadcast : 192.168.1.127	ID Host más alto : 192.168.1.126	

Tabla B-9 Subred 3

	NÚMERO DE RED	**VALOR BIT ÚLTIMO OCTETO**
Dirección IP	192.168.1	128
Dirección IP (Binario)	11000000.10101000.00000001	**10**000000
Máscara de subred (Binario)	11111111.11111111.11111111	**11**000000
Dirección de Subred : 192.168.1.128	ID Host más bajo : 192.168.1.129	
Dirección de Broadcast : 192.168.1.191	ID Host más alto : 192.168.1.190	

Tabla B-10 Subred 4

	NÚMERO DE RED	**VALOR BIT ÚLTIMO OCTETO**
Dirección IP	192.168.1	0

<table>
<tr><td>Dirección IP (Binario)</td><td colspan="2">11000000.10101000.00000001</td><td>11000000</td></tr>
<tr><td>Máscara de subred (Binario)</td><td colspan="2">11111111.11111111.11111111</td><td>11000000</td></tr>
<tr><td colspan="2">Dirección de Subred : 192.168.1.192</td><td colspan="2">ID Host más bajo : 192.168.1.193</td></tr>
<tr><td colspan="2">Dirección de Broadcast : 192.168.1.255</td><td colspan="2">ID Host más alto : 192.168.1.254</td></tr>
</table>

Ejemplo de Ocho Subredes

De forma similar se puede utilizar una máscara de 27 bits para crear 8 subredes (001,010,011,100,101,110)

La siguiente tabla muestra el último octeto de la dirección IP clase C para cada subred.

Tabla B-11 Ocho Subredes

SUBRED	DIRECCIÓN SUBRED	PRIMERA DIRECCIÓN	ÚLTIMA DIRECCIÓN	DIRECCIÓN BROADCAST
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

La siguiente tabla resume el plan de subredes de clase “C”.

Tabla B-12 Plan de Subred Clase C

Nº BITS “PRESTADOS”	MÁSCARA DE SUBRED	Nº SUBREDES	Nº HOSTS POR SUBRED
1	255.255.255.128(/25)	2	126
2	255.255.255.192(/26)	4	62

3	255.255.255.224(/27)	8	30
4	255.255.255.240(/28)	16	14
5	255.255.255.248(/29)	32	6
6	255.255.255.252(/30)	64	2
7	255.255.255.254(/31)	128	1

Subredes con Redes Clase A y Clase B

Para direcciones clase “A” y clase “B”, la máscara de subred también determina que bits forman parte del número de red y cuáles parte del identificador de host.

Una dirección clase “B” tiene dos octetos para el identificador de host y una dirección clase “A” tiene tres octetos para la identificación de host disponibles para subredes.

La siguiente tabla resume el plan de subredes para la clase “B”.

Tabla B-13 Plan de Subredes en Clase B

Nº BITS “PRESTADOS”	MÁSCARA DE SUBRED	Nº SUBREDES	Nº HOSTS POR SUBRED
1	255.255.128.0(/17)	2	32766
2	255.255.192.0(/18)	4	16382
3	255.255.224.0(/19)	8	8190
4	255.255.240.0(/20)	16	4094
5	255.255.248.0(/21)	32	2046
6	255.2555.252.0(/22)	64	1022
7	255.255.254.0(/23)	128	510
8	255.255.255.0(/24)	256	254
9	255.255.255.128(/25)	512	126
10	255.255.255.192(/26)	1024	62
11	255.255.255.224(/27)	2048	30

12	255.255.255.240(/28)	4096	14
13	255.255.255.248(/29)	8192	6
14	255.255.255.252(/30)	16384	2
15	255.255.255.254(/31)	32768	1

Apéndice C

Wireless LAN e IEEE 802.11

Una wireless LAN (WLAN) proporciona un sistema de comunicaciones de datos flexible que puede utilizar para acceder a varios servicios (navegar por Internet, correo electrónico, impresoras, etc.) sin el coste de ninguna estructura de red cableada. En efecto un entorno wireless LAN le proporciona la libertad de permanecer conectado a la red en el área de cobertura.

Beneficios de una Wireless LAN

1. Acceso a servicios de red en áreas donde resulta difícil o muy caro cablear, como edificios históricos, edificios con materiales asbestos y aulas.
2. Doctores y enfermeras pueden acceder al perfil completo de un paciente con un dispositivo portátil al entrar en la habitación del paciente.
3. Permite a los grupos de trabajo ser flexibles, al suponer un bajo coste total de propiedad para redes que son reconfiguradas frecuentemente.
4. Usuarios de salas de conferencias pueden acceder a la red cuando se mueven de una reunión a otra accediendo a información actualizada, lo que facilita la comunicación de decisiones instantánea.
5. Proporciona cobertura de red en todo un campus, permitiendo a las empresas la capacidad de roaming colocar redes wireless de fácil manejo que cubren de forma transparente un campus entero.

IEEE 802.11

La conclusión de 1997 del estándar IEEE 802.11 para wireless LANs (WLANs) fue un primer paso importante en el desarrollo evolutivo de las tecnologías de redes wireless. El estándar fue desarrollado para maximizar la interoperabilidad entre diferentes marcas de wireless LANs y para implantar variedad de mejoras de resultados y beneficios. El 16 de Septiembre de 1999, el 802.11b proporcionaba tasas de datos mucho más altas de hasta 11Mbps, manteniendo el protocolo 802.11.

El IEEE 802.11 especifica tres métodos de transmisión diferentes para el PHY, la capa responsable para transferir datos entre nodos. Dos de los métodos utilizan señales de RF de amplio espectro, Direct Sequence Spread Spectrum (DSSS) y Frequency-Hopping Spread Spectrum (FHSS), en la banda de 2.4 a 2.4825 GHz, banda sin licencia llamada ISM (Industrial, Scientific and Medical). El tercer método es tecnología de infrarrojo, utilizando frecuencias muy altas, justo por debajo de la luz visible en el espectro electromagnético para transportar datos.

Configuración de Wireless LAN PC a PC (Ad-hoc)

La configuración WLAN más simple es una WLAN independiente que conecta un conjunto de PCs con nodos wireless o estaciones (STA), lo que se denomina Basic Service Set (BSS). En la mayoría de las formas básicas, una wireless LAN conecta un conjunto de PCs con adaptadores wireless. Cada vez que dos o más adaptadores wireless están dentro del rango del otro, pueden formar una red independiente, a lo que se denomina comúnmente como red Ad-hoc o Independent Basic Service Set (IBSS). Vea el siguiente diagrama de un ejemplo de una wireless LAN PC a PC.



Diagrama C-1 Comunicación en una red PC a PC

Configuración Wireless LAN con punto de acceso

En este tipo de WLANs denominadas Infraestructure, múltiples puntos de acceso (APs) enlazan la WLAN a la red cableada y permiten a los usuarios compartir eficientemente los recursos de la red. Los puntos de acceso no proporcionan solamente comunicación con la red cableada pero también actúan como mediadores del tráfico de red wireless en entornos cercanos. Múltiples puntos de acceso pueden proporcionar cobertura wireless para un edificio o un campus entero. Todas las comunicaciones entre estaciones o entre una estación y una red cableada van a través del punto de acceso.

El Extended Service Set (ESS) que se muestra a continuación consta de una serie de BSSs que se solapan (cada una con un punto de acceso) conectadas entre sí por medio de un Distribution System (DS). Aunque el DS podría ser cualquier tipo de red, casi siempre es una Ethernet LAN. Los nodos móviles pueden cambiar de punto de acceso y se obtiene una cobertura en la zona de forma transparente.

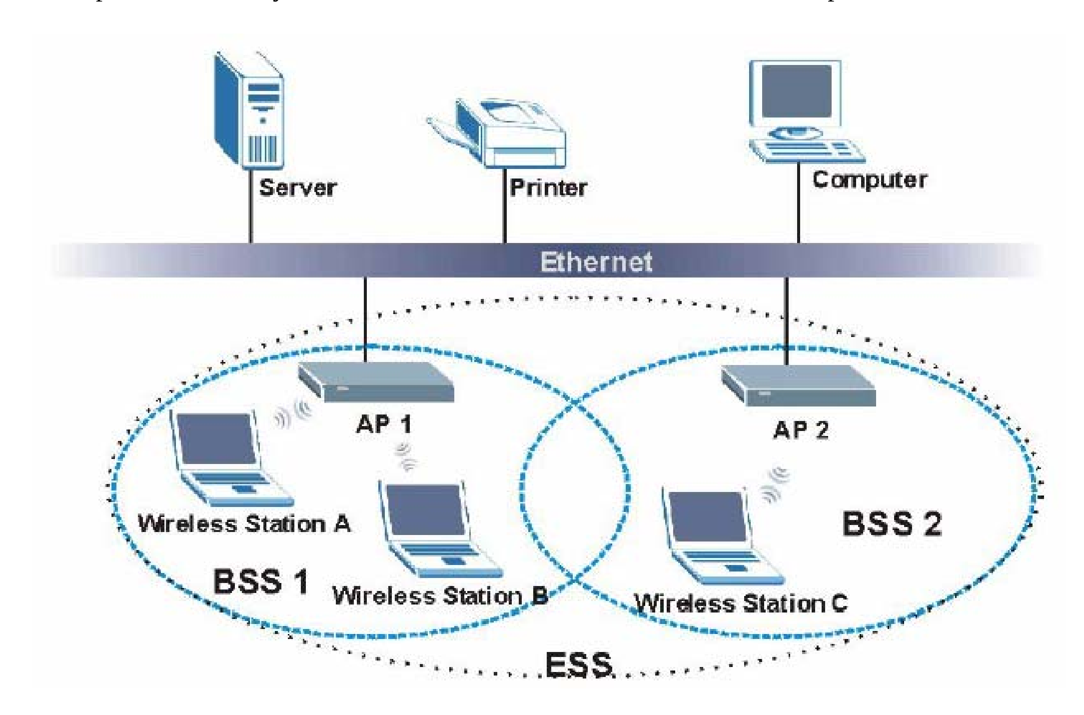


Diagrama C-2 ESS Proporciona Cobertura en una Zona

Apéndice D
PPPoE

PPPoE en Acción

Un módem ADSL establece una sesión PPP sobre Ethernet (PPP sobre Ethernet, RFC 2516) de su PC a un ATM PVC (Permanent Virtual Circuit, Circuito Permanente Virtual) que se conecta a un concentrador de acceso xDSL donde termina la sesión PPP (vea la siguiente figura). Un PVC puede soportar un número indeterminado de sesiones PPP iniciadas en la LAN. PPPoE proporciona las funcionalidades de control de acceso y de tarificación de forma similar a los servicios telefónicos usando PPP.

Beneficios de PPPoE

PPPoE ofrece los siguientes beneficios:

1. Le proporciona una interfaz de usuario familiar similar al de la red telefónica (DUN).
2. Reduce la carga de las portadoras en el aprovisionamiento de los circuitos virtuales que tienen que hacer los ISP en sus dispositivos para miles de usuarios.
3. Permite al ISP utilizar el modelo existente de la red telefónica para autentificar y (opcionalmente) proporcionar servicios diferenciados.

Escenario Tradicional

El siguiente diagrama representa una configuración hardware típico donde los PCs usan la red tradicional de marcado.

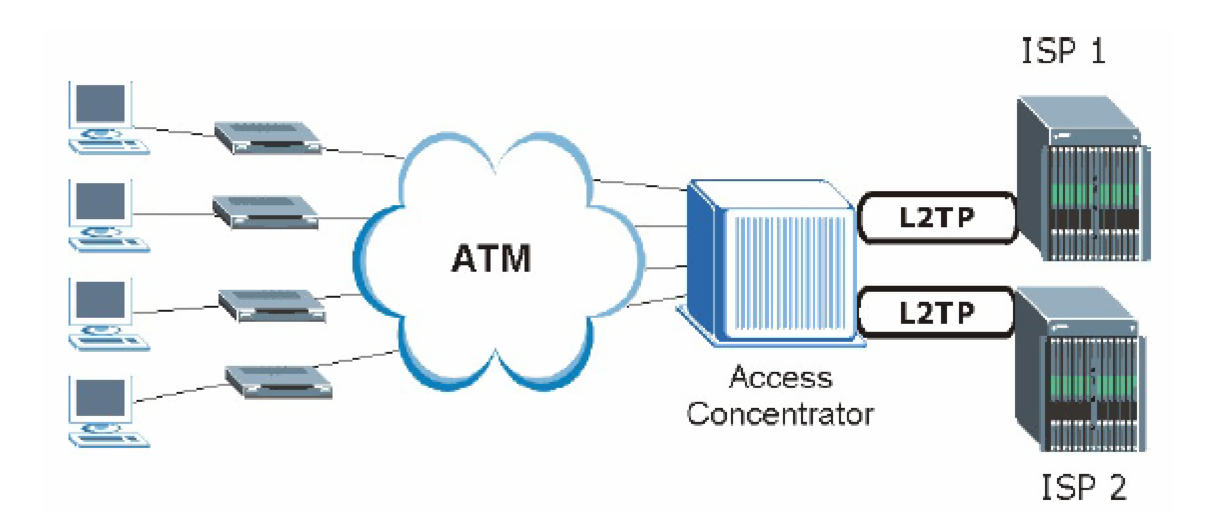


Diagrama D-1 Configuración Router monopuesto

Cómo funciona PPPoE

El driver PPPoE hace que la Ethernet aparezca como un enlace serie al PC y el PC ejecuta el PPP, mientras que el modem puentea las tramas Ethernet al Concentrador de Acceso (AC). Entre el concentrador y un ISP, el concentrador actúa como L2TP (Protocolo de Tunneling de Nivel 2) LAC (L2TP Access Concentrator) y sirve de túnel entre los tramas PPP y el ISP. El túnel L2TP es capaz de transportar multitud de sesiones PPP.

Con PPPoE, el circuito virtual (VC) es equivalente a la conexión de marcado telefónico y es entre el modem y el AC. Sin embargo, la negociación PPP es entre el PC y el ISP.

El Prestige como un Cliente PPPoE

Cuando utilice el Prestige como un cliente PPPoE, los PCs de la LAN solamente ven la Ethernet y no son conscientes de la presencia de PPPoE. Esto evita que el administrador tenga que gestionar clientes PPPoE en PCs individuales.

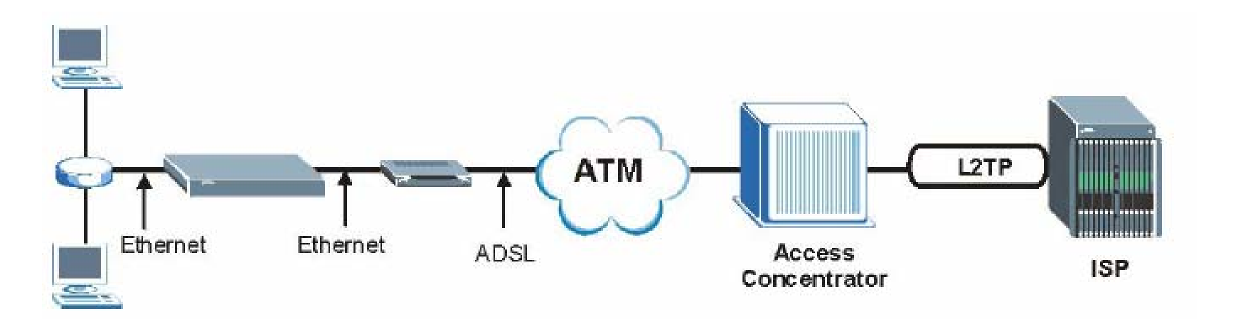


Diagrama D-2 El Prestige como un Cliente PPPoE

Apéndice E

Topología de Circuito Virtual

ATM es una tecnología orientada a conexión, lo que significa que establece circuitos virtuales a través de los cuales se comunican los sistemas finales. La terminología para circuitos virtuales es la siguiente:

• Virtual Channel (Canal Virtual)	Conexiones lógicas entre switches ATM
• Virtual Path (Camino Virtual)	Un haz de canales virtuales
• Virtual Circuit (Circuito Virtual)	Una serie de caminos virtuales entre puntos finales de circuitos

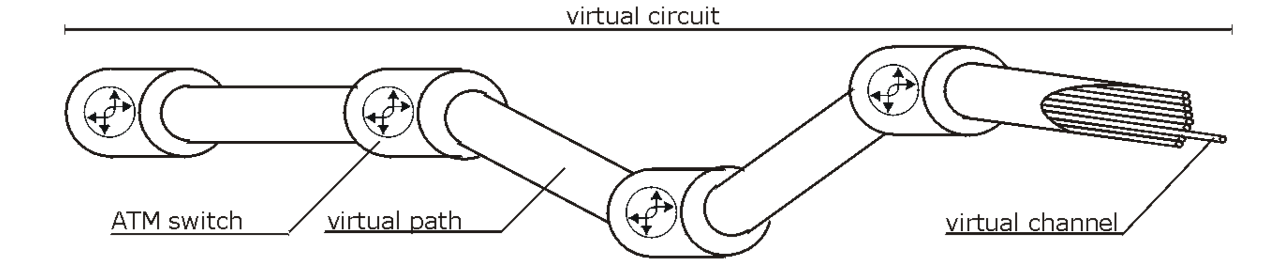


Diagrama 1 Topología de Circuito Virtual

Piense en un camino virtual como un cable que contiene un haz de cables en su interior. El cable conecta dos puntos y los cables de dentro proporcionan circuitos individuales entre los dos puntos. En una cabecera de paquete ATM, un VPI (Identificador de Camino Virtual) identifica un enlace formado por un camino virtual; un VCI (Identificador de Canal Virtual) identifica un canal dentro de un camino virtual.

El VPI y VCI identifican a un camino virtual, esto es, puntos de terminación entre switches ATM. Una serie de caminos virtuales conforman un circuito virtual.

Su proveedor de servicios debería suministrarle los números de VPI y VCI.

Apéndice F
Configuración de la dirección IP de su PC

Todos los PCs deben tener una tarjeta adaptadora Ethernet 10M o 100M y el TCP/IP instalado.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 y sistemas operativos posteriores y todas las versiones de UNIX/LINUX incluyen los componentes software que necesita para instalar y utilizar TCP/IP en su PC. Windows 3.1 requiere la compra de un paquete de la aplicación TCP/IP.

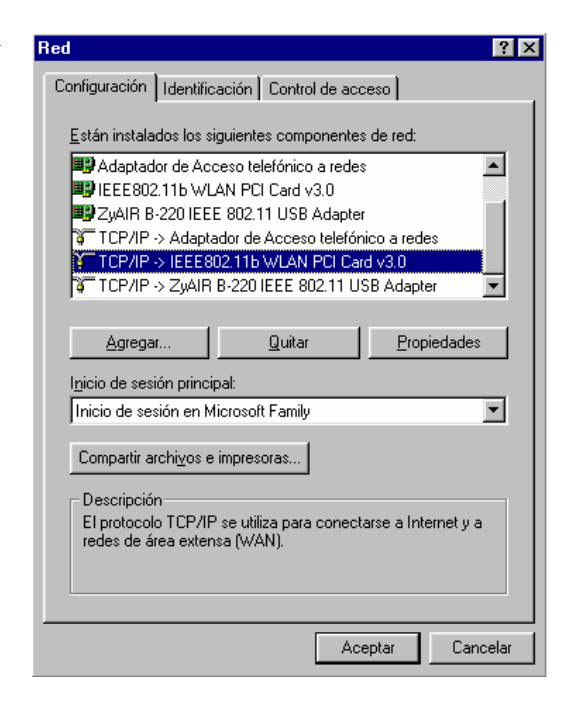
TCP/IP ya debería estar instalado en los ordenadores que emplean Windows NT/2000/XP, Macintosh OS 7 y sistemas operativos posteriores.

Después de haber instalado los componentes TCP/IP apropiados, configure el TCP/IP para "comunicarse" con su red.

Si asigna manualmente la información IP en lugar de utilizar asignación dinámica, asegúrese de que sus PCs tienen direcciones IP que los sitúan en la misma subred que el puerto LAN del Prestige.

Windows 95/98/Me

Haga clic en **Inicio**, **Configuración**, **Panel de Control** y luego doble clic en el icono **Red** para abrir la ventana de **Red**.



Instalar Componentes

La pestaña **Configuration** de la ventana **Network** muestra una lista de los componentes instalados. Necesita un adaptador de red, el protocolo TCP/IP y un Cliente para Redes Microsoft.

Si necesita el adaptador:

a. En la ventana **Red**, haga clic en **Agregar**.

b. Seleccione **Adaptador** y luego haga clic en **Agregar**.

c. Seleccione el fabricante y modelo del adaptador de red y haga clic en **OK**.

Si necesita el TCP/IP:

a. En la ventana **Red**, haga clic en **Agregar**.

b. Seleccione **Protocolo** y luego haga clic en **Agregar**.

c. Seleccione **Microsoft** en la lista de fabricantes.

d. Seleccione **TCP/IP** en la lista de protocolos de red y haga clic en **OK**.

Si necesita Cliente para Redes Microsoft:

a. Haga clic en **Agregar**.

b. Seleccione **Cliente** y luego haga clic en **Agregar**.

c. Seleccione **Microsoft** en la lista de fabricantes.

d. Seleccione **Cliente para Redes Microsoft** en la lista de clientes de red y haga clic en **OK**.

e. Reinicie su PC para que los cambios realizados surtan efecto.

Configurar

1. En la pestaña de **Configuración** de la ventana **Red,** seleccione la entrada de TCP/IP de su adaptador de red y haga clic en **Propiedades**.

2. Seleccione la pestaña **Dirección IP**.

   -Si su dirección IP es dinámica, seleccione **Obtener una dirección IP automáticamente**.

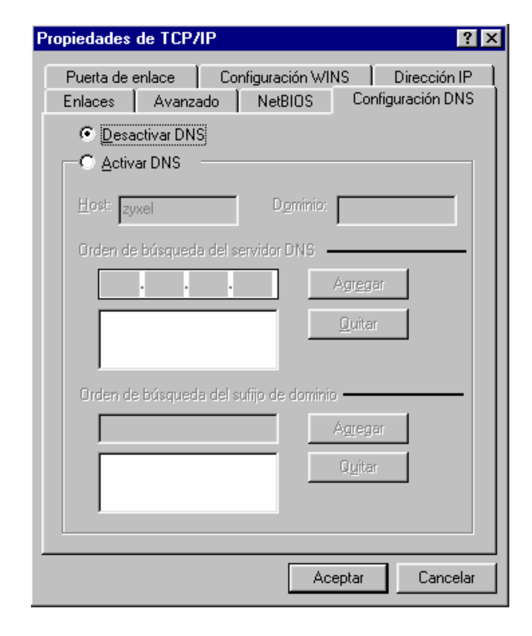
   -Si tiene una dirección IP estática, seleccione **Especificar una dirección IP** e introduzca la información correspondiente en los campos **Dirección IP** y **Máscara de Subred**.



3. Vaya a la pestaña **Configuración DNS**.

   -Si no conoce la información de su DNS, seleccione **Desactivar DNS**.

   -Si conoce esa información, seleccione **Activar DNS** e introduzca la información en los campos siguientes (quizá no necesite rellenarlos todos).



4. Haga clic en la pestaña **Puerta de enlace**.

   -Si no conoce la dirección IP de su gateway, quite previamente los gateways instalados.

   -Si tiene una dirección IP del gateway, introdúzcalo en el campo **Nueva puerta de enlace** y haga clic en **Agregar**.



5. Haga clic en **Aceptar** para guardar y cerrar la ventana **Propiedades TCP/IP**.

6. Haga clic en **Aceptar** para cerrar la ventana **Red**. Inserte el CD de Windows si le es solicitado.

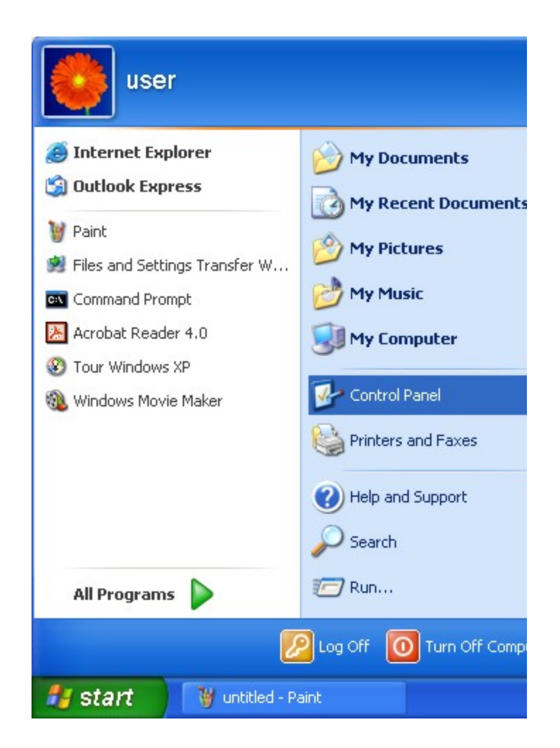
7. Encienda el Prestige y reinicie su PC cuando se le solicite.

Verificar Configuración

1. Haga clic en **Inicio** y luego en **Ejecutar**.
2. En la ventana **Ejecutar**, teclee "winipcfg" y pulse **Aceptar** para abrir la ventana **Configuración IP**.
3. Seleccione el adaptador de red. Debería ver la dirección IP de su ordenador, la máscara de subred y el gateway por defecto.

Windows 2000/NT/XP

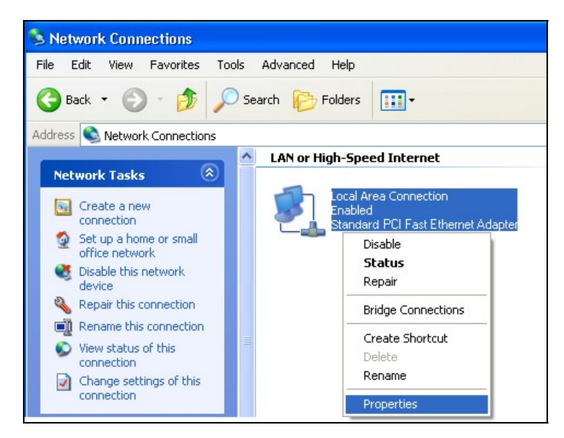
1. Si usa Windows XP, haga clic en **Inicio**, **Panel de Control**. En Windows 2000/NT, haga clic en **Inicio**, **Configuración**, **Panel de Control**.



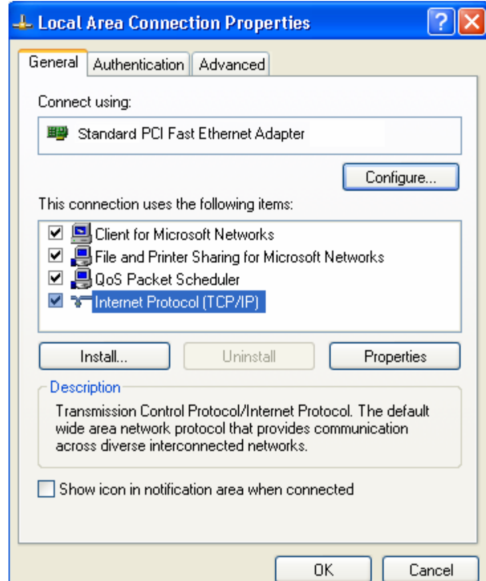
2. En Windows XP, haga clic en **Conexiones de Red**. En Windows 2000/NT, clic en **Conexiones de Red y de Acceso Telefónico**.



3. Haga clic con el botón derecho en **Conexión de Área Local** y luego haga clic en **Propiedades**.



4. Seleccione **Protocolo Internet (TCP/IP)** (en la pestaña **General** en XP) y pulse **Propiedades**.

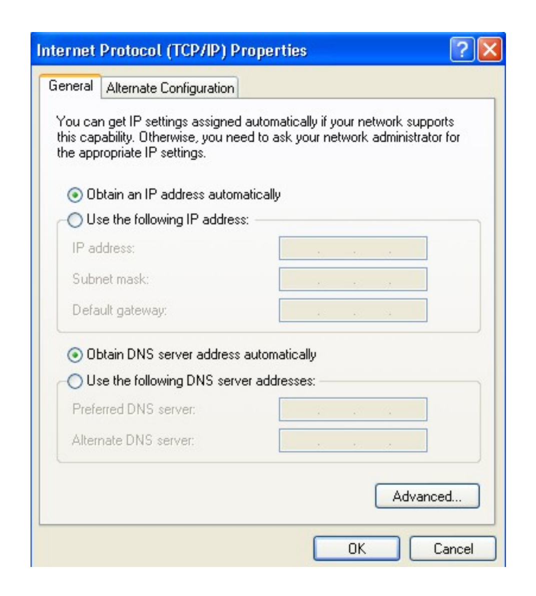


5. Se abre la ventana **Protocolo Internet TCP/IP Propiedades** (la pestaña **General** en Windows XP).

   -Si tiene una dirección IP dinámica, haga clic en **Obtener una dirección IP automáticamente**.

   -Si tiene una dirección IP estática, haga clic en **Usar la siguiente dirección IP** y rellene los campos **Dirección IP**, **Máscara de subred** y **Puerta de enlace predeterminada**.

   Haga clic en **Avanzada**.



6. -Si conoce la dirección IP de su gateway, quite cualquier gateway que haya sido instalado previamente en pestaña **Configuración de IP** y pulse **Aceptar**.

   Siga estos pasos para configurar direcciones IP adicionales:

   -En la pestaña **Configuración de IP**, en direcciones IP, haga clic en **Agregar**.

   -En **Direcciones IP**, introduzca la dirección IP en **dirección IP** y la máscara de subred en **Máscara de subred**, y luego haga clic en **Agregar**.

   -Repita los dos pasos anteriores para cada dirección IP que desee añadir.

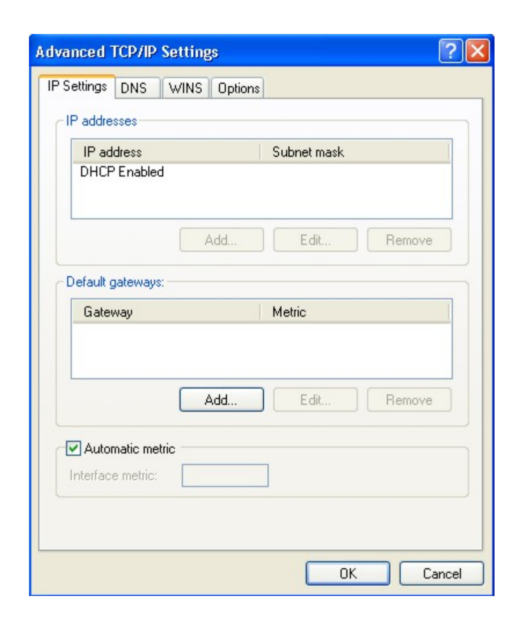
   -Configure más gateways por defecto en la pestaña **Configuración de IP** haciendo clic en **Agregar** en **Puertas de enlace predeterminadas**.

   -Introduzca la dirección IP del gateway por defecto en **Puerta de enlace**. Para configurar manualmente una métrica por defecto (el número de saltos de transmisión), borre la opción **Métrica automática** e introduzca un valor en **Métrica**.

   -Haga clic en **Agregar**.

   -Repita los tres pasos anteriores para cada gateway por defecto que quiera agregar.

   -Haga clic en **Aceptar** cuando acabe.

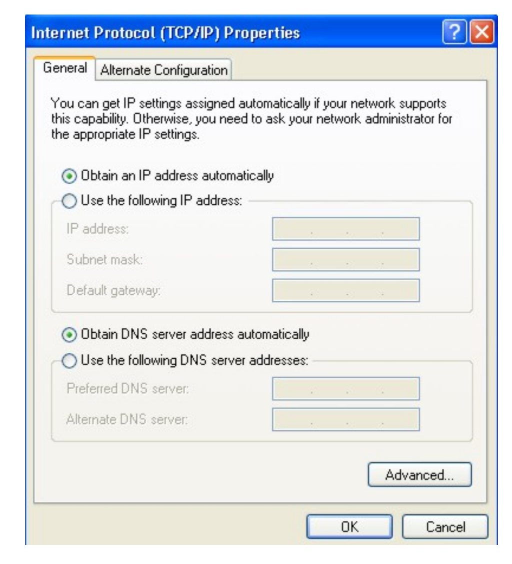


7. En la ventana **Protocolo Internet TCP/IP Propiedades** (la pestaña **General** en Windows XP):

   -Haga clic en **Obtener la dirección del servidor DNS automáticamente** si no sabe la(s) dirección(es) de su servidor DNS.

   -Si sabe la(s) dirección(es) de su servidor DNS, haga clic en **Usar las siguientes direcciones de servidor DNS**, e introdúzcalos en los campos **Servidor DNS preferido** y **Servidor DNS alternativo**.

   Si han configurado previamente servidores DNS, haga clic en **Avanzada** y seleccione la pestaña **DNS** para ordenarlos.



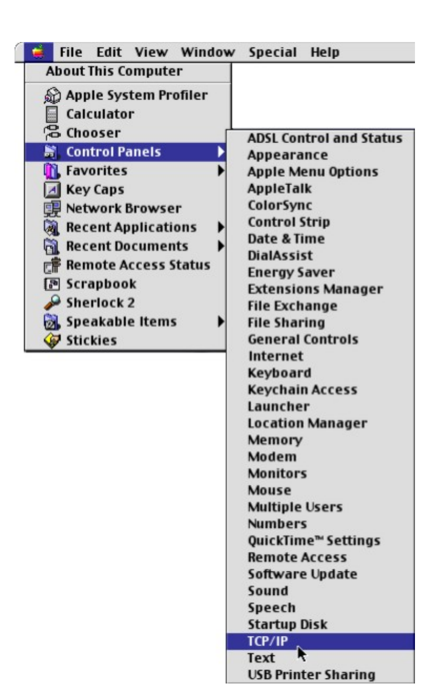
8. Haga clic en **Aceptar** para cerrar la ventana de **Propiedades de Protocolo Internet (TCP/IP)**.
9. Haga clic en **Aceptar** para cerrar la ventana de **Propiedades de Conexión de Área Local**.
10. Encienda su Prestige y reinicie su PC (si le es solicitado).

Verificar Configuración

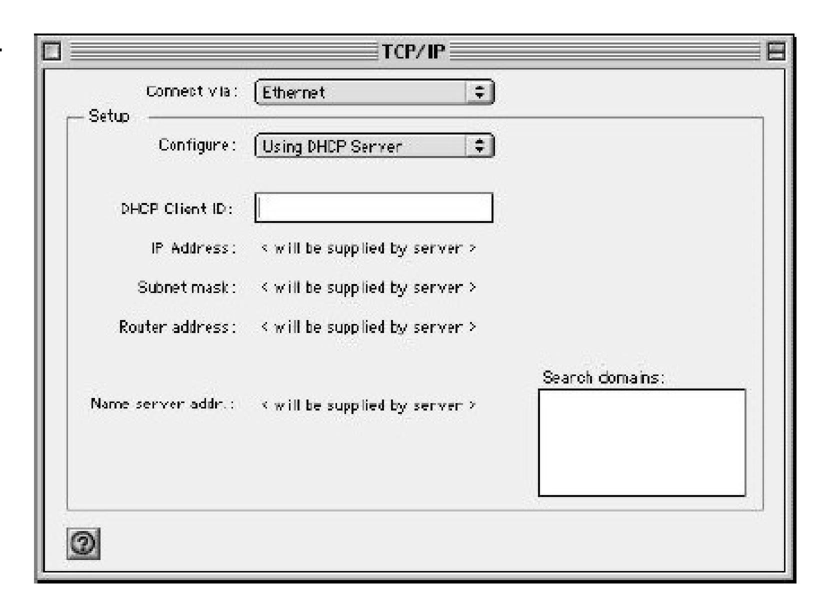
1. Haga clic en **Inicio**, **Programas**, **Accesorios** y luego **Símbolo del Sistema**.
2. En la ventana **Símbolo del sistema**, teclee "ipconfig" y luego pulse [ENTER]. También puede abrir **Conexiones de Red**, haga clic con el botón derecho en una conexión de red, haga clic en **Estado** y luego en la pestaña **Compatibilidad**.

Macintosh OS 8/9

1. Haga clic en el menú **Apple**, **Control Panels** y haga doble clic en **TCP/IP** para abrir **TCP/IP Control Panel**.



2. Seleccione **Ethernet built-in** de la lista de **Connect via**.



3. Para configuraciones asignadas dinámicamente, seleccione **Using DHCP Server** de la lista **Configure:**.
4. Para configuraciones asignadas estáticamente, haga lo siguiente:

   -De la caja **Configure**, seleccione **Manually**.

   -Introduzca su dirección IP en la caja **IP Address**.

   -Introduzca su máscara de subred en la caja **Subnet mask**.

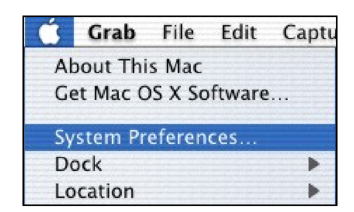
   -Introduzca la dirección IP de su Prestige en la caja **Router address**.
5. Cierre el **TCP/IP Control Panel**.
6. Haga clic en **Save** si le es solicitado, para guardar los cambios de su configuración.
7. Encienda su Prestige y reinicie su ordenador (si se le pide).

Verificar Configuración

Compruebe las propiedades del TCP/IP en la ventana **TCP/IP Control Panel**.

Macintosh OS X

1. Haga clic en el menú **Apple**, y haga clic en **System Preferences** para abrir la ventana **System Preferences**.

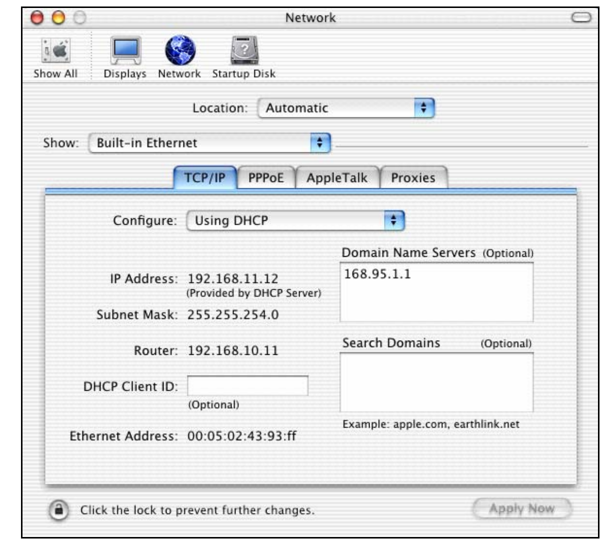


2. Haga clic en **Network** en la barra de iconos.

   - Seleccione **Automatic** de la lista **Location**.

   - Seleccione **Built-in Ethernet** de la lista **Show.**

   - Haga clic en la pestaña **TCP/IP**.



3. Para configuraciones asignadas dinámicamente, seleccione **Using DHCP** de la lista **Configure**.
4. Para configuraciones asignadas estáticamente, haga lo siguiente:

   -En **Configure**, seleccione **Manually**.

   -Introduzca su dirección IP en **IP Address**.

   -Introduzca la máscara de subred en **Subnet mask**.

   -Introduzca la dirección IP del Prestige en **Router address**.
5. Haga clic en **Apply Now** y cierre la ventana.
6. Encienda el Prestige y reinicie su PC (si se le solicita).

Verificar Configuración

Compruebe las propiedades TCP/IP en la ventana **Red**.